

Diplomarbeit im Studiengang Medieninformatik

Terminal Services: Funktionalität, Einsatzgebiete,
Alternativen, Trends und der praktische Einsatz in einer
webbasierten Umgebung bei der Firma Linde

vorgelegt von Sebastian Dommel
an der Hochschule der Medien Stuttgart
am 15.9.2006 (Abgabetermin)

Erstprüfer: Prof. Walter Kriha
Zweitprüfer: Dr. Gabriele Engl

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbständig und ohne fremde Hilfe angefertigt zu haben. Die verwendete Literatur und sonstige Hilfsmittel sind vollständig angegeben.

Stuttgart,

Abstract

Server Based Computing ist nach Zahlen des European Thin Client Forums eine erfolgreiche Wachstumsbranche mit Wachstumsraten von ca. 35 Prozent. Eine wichtige Form des Server Based Computing sind die Terminal Services. Terminal Services und Citrix Umgebungen sind sehr beliebt, wenn es darum geht Applikationen zentral auf einem Server zu verwalten und laufen zu lassen. Die Vorteile liegen auf der Hand: Geringerer Administrationsaufwand, Einsparung von Lizenzkosten, und Mobilität der Benutzer.

Je nach Firmengröße, Anzahl und Art der Anwendungen und der allgemeinen Strategie im Unternehmen sind allerdings traditionelle Netzwerke mit Desktop PCs, in denen die Wartung durch automatische Softwareverteilung vereinfacht werden kann, vorzuziehen.

Die Arbeit gibt einen Überblick über die Funktionsweise und Anwendungsgebiete der Terminal Services. Es werden Entwicklungen und Alternativen, wie der Einsatz von Blades, die Virtualisierung von Applikationen und des Betriebssystems, sowie das Streaming von Applikationen vorgestellt und ihre Auswirkungen auf die Terminal Services bewertet. Zusätzlich werden Lösungen zum sicheren Zugang über das Internet durch Verschlüsselung und Endpunktkontrolle vorgestellt.

In einem Ausblick sind mögliche Konsequenzen der Veröffentlichung des neuen Betriebssystems Vista bzw. der Servervariante Longhorn aufgezeigt und Trends, wie z.B. die Weiterentwicklungen bei der Messung und Steigerung der Performanz von Terminal Server Systemen beschrieben.

Der praktische Teil der Arbeit besteht aus der Erstellung eines Webportals für spezielle IT-Applikationen (Prozess Design Programme), das im Geschäftsbereich Linde Engineering der Linde AG in Pullach bei München verwendet wird. Bei diesem konkreten Anwendungsbeispiel für Terminal Services werden in einem webbasierten Portal Applikationen in einer Citrix Umgebung und zugehörige Informationen gebündelt und für externe Benutzer in Tochter- oder Partnerfirmen weltweit und Mitarbeiter auf Reisen zur Verfügung gestellt.

Nach Analyse der Ausgangssituation durch Zusammenführen der Anforderungen und der Erfassung der Rahmenbedingungen, werden Potentiale und Optionen von verschiedenen Lösungen aufgezeigt und die Umsetzung der Applikation beschrieben.

Abkürzungsverzeichnis

AAC	=	Advanced Access Control
ACE	=	Assured Computing Environment
AIE	=	Application Isolation Environment
ASP	=	Active Server Pages
CPU	=	Central Processing Unit
DLL	=	Dynamic Link Library
DMZ	=	Demilitarized Zone
EMF	=	Enhanced Metafile Format
ETCF	=	European Thin Client Forum
HTTP	=	HyperText Transfer Protocol
HTML	=	Hypertext Markup Language
ICA	=	Independent Computing Architecture
IP	=	Internet Protocol
IPSec	=	Internet Protocol Security
ISS	=	Internet Information Services
IT	=	Informationstechnologie
J2EE	=	Java 2 Platform Enterprise Edition
MSI	=	Microsoft Installer
NAT	=	Network Address Translation
NIC	=	Network Interface Card
NLB	=	Network Load Balancing
OSI	=	Open Systems Interconnection
PC	=	Personal Computer
RDP	=	Remote Desktop Connection
RDP	=	Remote Desktop Protocol
SMS	=	Systems Management Server
SSL	=	Secure Socket Layer
TCO	=	Total Cost of Ownership

XAML	=	eXtensible Application Markup Language
XML	=	Extensible Markup Language
URL	=	Uniform Resource Locator
USB	=	Universal Serial Bus
VDI	=	Virtual Desktop Infrastructure
VPN	=	Virtual Private Network
WAN	=	Wide Area Network
WinFX	=	Windows Framework
WPF	=	Windows Presentation Foundation

Inhaltsverzeichnis

Inhaltsverzeichnis	3
1 Einleitung	5
2 Terminal Services	8
2.1 Überblick	8
2.2 Geschichte	9
2.3 Funktionalität	11
2.4 Technische Funktionsweise	18
2.4.1 Mehrbenutzer Betriebssystem	18
2.4.2 Präsentationsprotokoll	20
2.4.3 Netzwerkarchitektur	23
2.5 Vergleich der Terminal Services mit anderen Architekturen	26
2.5.1 Vor- und Nachteile der Terminal Services	26
2.5.2 Vor- und Nachteile Personal Computers	28
2.5.3 Vor- und Nachteile automatische Softwaredistribution	29
2.6 Anwendungsszenarien für Terminal Server	31
2.6.1 Thin Clients	31
2.6.2 Remote und Mobile Computing	32
2.6.3 Application Service Providing	34
3 Entwicklungen im Bereich des Server Based Computing	36
3.1 Virtualisierung	37
3.1.1 Servervirtualisierung	37
3.1.2 Applikationsvirtualisierung	43
3.2 Blade Technologie	45
3.2.1 Blade Server	45
3.2.2 Bladed PC	47

3.3	Streaming Technologie	49
3.4	Secure und Smart Access	54
3.5	Bewertung der Technologien im Überblick	60
4	Ausblick	62
4.1	Mircosoft Longhorn Server	62
4.2	Mircosoft Vista Presentation Layer	64
4.3	Performance Measuring und Traffic Shaping	65
5	Die Firma Linde	69
5.1	Der Konzern	69
5.2	Linde Engineering	70
5.3	Der Bereich Informatik	71
5.4	Abteilung "Informatik für Verfahrenstechnik"	72
6	Prozess Design Portal	74
6.1	Kurzbeschreibung	74
6.2	Funktionalität	75
6.3	Ziele	76
6.4	Technologieauswahl	77
6.4.1	Citrixumgebung	77
6.4.2	Portalserver	80
6.4.3	Webserver	82
6.4.4	Java	83
6.5	Umsetzung	84
7	Fazit	94
	Abbildungsverzeichnis	96
	Literaturverzeichnis	99

Kapitel 1

Einleitung

Server Based Computing ist eine erfolgreiche Wachstumsbranche. Nach Zahlen des European Thin Client Forums wuchs der Markt von Thin Client Einheiten in den letzten zwei Jahre von ca. 35 Prozent (vgl. [For05](#)). Nahezu alle Firmen des Fortune 500 Indexes nutzen Server Based Computing in Form von Terminal Servern und der Software des erfolgreichsten Zusatzanbieters Citrix in ihrem Unternehmen (vgl. [Cit06b](#)).

Oder, wie es treffend in einem Online Artikel stand: "Server Based Computing boomt - und niemand spricht darüber" (vgl. [Tei05](#)). Denn es wird wenig über diese Thematik geredet oder geschrieben, obwohl, wenn man den Anbietern glauben darf, weltweit alle großen Unternehmen diese Technologie einsetzen.

Eine wichtige Form des Server Based Computing sind die Terminal Services. Die Diplomarbeit wird das Konzept von Terminal Services vorstellen, den aktuellen Entwicklungsstand beleuchten und eine Abwägung zu anderen konkurrierenden Technologien, sowie neuen Trends, vornehmen.

Terminal Services und Citrix Umgebungen sind sehr beliebt, wenn es darum geht Applikationen zentral auf einem Server zu verwalten und laufen zu lassen. Die Vorteile liegen auf der Hand: Geringerer Administrationsaufwand, Einsparung von Lizenzkosten und Mobilität der Benutzer.

Eine Entscheidung für die Terminal Server Architektur kann in vielen Fällen Vorteile bringen. Doch der jeweilige Business Case entscheidet letztlich darüber, ob Terminal Services Sinn machen, oder ob ein Einsatz von neuen oder alternativen Technologien vorzuziehen ist.

Je nach Firmengröße, Anzahl und Art der Anwendungen und der allgemeinen Strategie im Unternehmen können z.B. traditionelle Netzwerke mit Desktop PCs, in

denen die Wartung durch automatische Softwareverteilung vereinfacht wird, sinnvoller sein.

Neue Entwicklungen, wie der Einsatz von Blades, die Virtualisierung von Applikationen und des Betriebssystems, sowie das Streaming von Applikationen können ein geeigneteres Konzept für die Bereitstellung von Desktops und Anwendungen für die Benutzer darstellen. Sie können aber auch Terminal Services ergänzen oder verbessern. Für jedes Unternehmen gibt es eine eigene beste Lösung.

Die Arbeit gibt einen Überblick über die Funktionsweise und Anwendungsgebiete der Terminal Services. Es werden die wichtigsten Punkte für und gegen einen Einsatz von Terminal Services aufgezeigt und es wird geklärt, in welchen Situationen diese nützlich sind und für welche Szenarien andere Technologien zu bevorzugen sind. Diese Alternativen zu Terminal Services werden zusammen mit ihren Vor- und Nachteilen in bestimmten Situationen vorgestellt.

Der Markt des Server Based Computing ist heiß umkämpft. Gerade große Firmen wie Microsoft haben mit ihren aktuellen Strategie-Entscheidungen einen großen Einfluss auf die Branche. Mit der Veröffentlichung des neuen Betriebssystems Vista bzw. der Servervariante Longhorn und der wachsenden Unterstützung von Virtualisierung setzt Microsoft führende Firmen wie Citrix stark unter Druck.

Der Innovationsdrang bewirkt Weiterentwicklungen bei der Messung und Steigerung der Performanz von Terminal Server Systemen, sowie beim sicheren Zugang über das Internet durch Verschlüsselung und Endpunktkontrolle.

Die Arbeit zeigt ein Bild der aktuellen Entwicklungen auf. Außerdem wird ein Ausblick gegeben, wie die Zukunft von Terminal Services und Server Based Computing im Allgemeinen aussehen könnte.

Der praktische Teil der Arbeit besteht aus der Erstellung eines Webportals für spezielle IT-Applikationen (Prozess Design Programme), das bei der Firma Linde in Pullach bei München verwendet wird. Bei diesem konkreten Anwendungsbeispiel für Terminal Services werden in einem webbasierten Portal Applikationen in einer Citrixumgebung und zugehörige Informationen wie z.B. Kontaktdaten oder Handbücher gebündelt und für externe Benutzer in Tochter- oder Partnerfirmen und für Mitarbeiter auf Reisen zur Verfügung gestellt.

Ziel ist dabei unter anderem eine Effizienzsteigerung und die Erweiterung des Nutzerkreises. Erreicht werden soll dies durch den einfachen Zugang zu Anwendungen und Informationen und durch die Attraktivität der Plattform. Dabei soll

der Wissensschutz gewährleistet bleiben, interne Daten mit großer Sorgfalt behandelt und eine transparente und einfache Administration möglich gemacht werden.

Nach Analyse der Ausgangssituation durch Zusammenführen der Anforderungen und der Erfassung der Rahmenbedingungen, werden Potentiale und Optionen von verschiedenen Lösungen aufgezeigt.

Die letzten Endes getroffene Entscheidung für die Beibehaltung einer Terminal Service Umgebung wird anhand der Anforderungen und der Bewertung der verschiedenen Optionen herausgearbeitet. Die Vorgehensweise bei der Technologieauswahl zwischen Portal- und Webservern und die Implementierung wird dokumentiert und die Gründe für die Beibehaltung der Citrix Umgebung beleuchtet.

Kapitel 2

Terminal Services

Dieses Kapitel behandelt den Dienst der Terminal Services für Windows Server, sowie Zusatzsoftware wie Citrix *Presentation Server*. Nach einem Überblick im nächsten Kapitel wird auf die Entwicklungsgeschichte von Terminal Services in Kapitel 2.2 eingegangen. Nachdem die Funktionalität (vgl. 2.3) und die technische Funktionsweise (vgl. 2.4) erklärt wurden, wird das Konzept der Terminal Services mit anderen Alternativen in Kapitel 2.5 verglichen. Abschließend wird der Einsatz von Terminal Services anhand von mehreren möglichen Szenarien in Kapitel 2.6 beschrieben.

2.1 Überblick

In dieser Arbeit werden Begriffe, Firmen und Produkte genannt, die alle im Bereich des Server Based Computing angesiedelt sind. Beim Server Based Computing handelt es sich um ein Modell, bei dem Anwendungen zu 100 Prozent auf dem Server installiert, verwaltet, unterstützt und ausgeführt werden.

Terminal Services ist eine Komponente des Windows Server Betriebssystems und sie ermöglicht die Durchführung von Server Based Computing. Mit Hilfe der Terminal Services wird das Windows Betriebssystem mehrbenutzerfähig und es können damit mehrere Benutzer gleichzeitig auf dem Server arbeiten (vgl. MO03, S.22). Die technische Funktionsweise des Mehrbenutzerbetriebs wird in Kapitel 2.4.1 beschrieben. Das Basisprodukt hierfür ist der Microsoft Terminal Server.

Um den Terminal Server nutzen zu können, muss die Terminal Service Funktionalität bei Windows Server 2000 bzw. Windows Server 2003 aktiviert werden. Es fallen Lizenzkosten pro Terminal Server und Benutzer an (vgl. Sch05).

Citrix ist neben z.B. Tarantella, die seit Juli 2005 zu Sun Microsystems gehören (vgl. [Mic05](#)), eine Firma, die Add-on Software für den Terminal Server anbietet. Der *Citrix Presentation Server* läuft nur im Zusammenhang mit einem Microsoft Terminal Server und setzt seine Funktionalität (wie in Kapitel [2.3](#) beschrieben) auf dem Basisprodukt von Microsoft auf. Für den *Presentation Server* fallen zusätzliche Lizenzkosten an. Somit muss also jeweils der Terminal Server und die Add-on Software lizenziert werden.

Citrix und Microsoft haben mit ICA (=Independent Computing Architecture) bzw. RDP (=Remote Desktop Protocol) jeweils ihr eigenes Protokoll entwickelt, um Bildschirminhalte des Servers an den Client zu übertragen und Steuerungskommandos wie Tastatureingaben zurück an den Server zu leiten. Eine genau Beschreibung der Funktionsweise findet sich in Kapitel [2.4.2](#).

Anbieter wie Igel oder Wyse bieten Thin Clients an, also Rechner mit sehr reduzierter Hardware- und Softwareausstattung, die in einer Terminal Server Umgebung eingesetzt werden können. Die Verwaltung dieser Clientgeräte wird mit Hilfe von Administrationssoftware vereinfacht. Auf den Einsatz von Thin Clients und die daraus resultierenden Folgen wird in Kapitel [2.6.1](#) eingegangen.

Terminal Services eignen sich für mehrere Anwendungsszenarien, von denen einige im Kapitel [2.6](#) beschrieben werden. Der Einsatz ist jedoch nicht immer sinnvoll und richtet sich nach der Gewichtung der Anforderungen in den einzelnen Unternehmen. Unterschiede und Vor- und Nachteile zu anderen Architekturen werden im Kapitel [2.5](#) aufgezeigt.

2.2 Geschichte

Selbst wenn mit Terminal Services die Komponente im Betriebssystem von Microsoft gemeint ist, beginnt die Geschichte im Grunde genommen mit der Gründung der Firma Citrix 1989. Der Firmengründer Ed Iacobucci wollte eine Multibenutzer Version des Betriebssystems OS/2 entwickeln, stieß bei IBM allerdings auf taube Ohren und gründete daraufhin seine eigene Firma. Das Produkt *Multiuser* für OS/2 war der erste Erfolg der Firma (vgl. [Lüd06](#), S.35).

Die wichtigste Weichenstellung für die aktuelle Situation erfolgte 1993, als Citrix den Windows NT Source Code von Microsoft lizenzierte und damit die bis heute

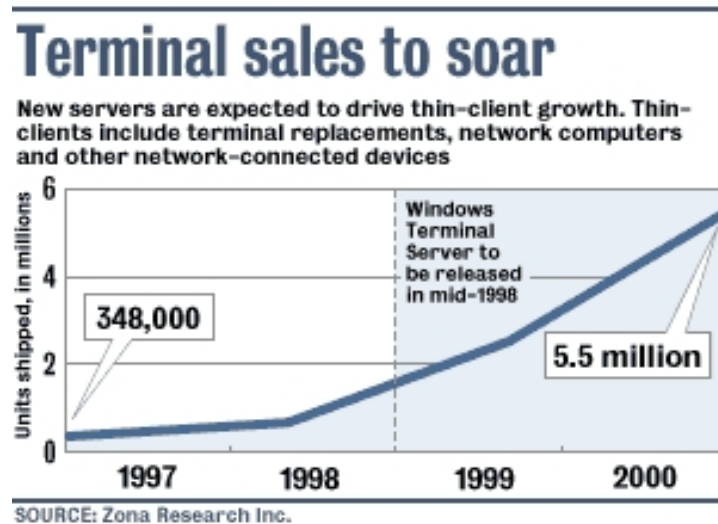


Abb. 2.1: Der Markt für Terminal Server entwickelte sich seit der ersten Veröffentlichung von Microsoft hervorragend.
Quelle: Zona Research

andauernde enge Zusammenarbeit beider Firmen begann. *WinFrame* war das erste, auf Windows NT 3.51 basierende, aber komplett eigenständige Produkt von Citrix, das Windows mehrbenutzerfähig machte (vgl. KH01, S.37).

1997 wurde mit der Unterzeichnung eines fünf Jahre dauernden Kooperationsvertrages zwischen Microsoft und Citrix der Weg für das erste Terminal Server Produkt von Microsoft geebnet. Citrix sah sich mehr oder weniger gezwungen sein Wissen an Microsoft weiterzugeben, um weiterhin Einblick in den Source Code von Windows NT zu erhalten. Microsoft lizenzierte die Citrix Technologie und veröffentlichte 1998 das noch eigenständige Produkt Windows Terminal Server Edition für Windows NT 4.0 (vgl. Tul05).

Citrix veröffentlichte im gleichen Jahr sein erstes Add-on Produkt *Metaframe* für den Microsoft Terminal Server. Da der Terminal Server nur absolute Basiskomponenten besaß und das ICA Protokoll von Citrix darüber hinaus dem RDP Protokoll von Microsoft sehr überlegen war, konnte Citrix sich erfolgreich am Markt als Zusatzanbieter etablieren.

Von diesem Zeitpunkt an begann Microsoft immer mehr Funktionen, die die *Metaframe* Versionen boten, selbst in das Terminal Server Basisprodukt zu integrieren und

den Vorsprung des ICA Prokolls immer weiter aufzuholen. Für die Version 2000 wurden die Terminal Services in das Standardprodukt Windows Server integriert (vgl. [Dre05](#), S.55 f.).

Aktuell hat Microsoft mit dem 2003 Release von Windows Server sein RDP Protokoll auf gleiche Augenhöhe mit dem ICA Protokoll gebracht, und die Terminal Services bieten genügend Funktionalität, sodass die Zusatzsoftware von Citrix, die nun *Presentation Server* heißt, nicht mehr in allen Fällen benötigt wird. Eine genaue Beschreibung der Funktionalität des Terminal Server bzw. des Citrix *Presentation Server* findet sich im nächsten Kapitel [2.3](#).

Die Ankündigungen von Microsoft, in der kommenden Version von Windows Server, mit dem Codenamen *Longhorn* die aktuellen Zusatzfunktionen von Citrix zu implementieren (siehe Kapitel [4.1](#)), veranlasst Citrix wie in den Jahren zuvor sich neue Innovationen zu überlegen, die einen Zusatz zum Microsoft Basisprodukt nötig machen (vgl. [Mad06b](#)).

Seit dem ersten Release hat sich die Zahl der eingesetzten Terminal Server explosionsartig erhöht (siehe Abbildung [2.1](#)). Durch die Integration von attraktiven Zusatzfunktionen, die zuvor nur durch andere Anbieter unterstützt wurden, steigert Microsoft weiterhin die Akzeptanz der Terminal Services.

2.3 Funktionalität

Microsoft Terminal Services bieten einen Grundsatz von Funktionalitäten, die hier aufgelistet und erklärt werden. Einige zum Teil wichtige Aspekte fehlen allerdings im Microsoft Produkt und können nur mit Software von anderen Anbietern abgedeckt werden. Diese Funktionalitäten werden im zweiten Teil dieses Kapitels besprochen.

Wichtige Funktionen des Terminal Servers sind:

- Der Mehrbenutzerbetrieb des Betriebssystems
- Das RDP Präsentationsprotokoll
- Die Installation und Freigabe von Applikationen
- Benutzerkonten und Gruppenrichtlinien
- Benutzerprofile

- Die Möglichkeit zu Drucken
- Das Session Shadowing
- Die Interaktion zwischen Client- und Server Umgebung

Die Grundfunktionalität des Terminal Servers ist der Mehrbenutzerbetrieb des Betriebssystems. Mehrere Clients können sich mit dem Server verbinden und gleichzeitig darauf arbeiten. Wie das technisch möglich ist, wird im Kapitel 2.4.1 erklärt.

Alle Aktionen, die der Benutzer ausführt und die Reaktion des Servers werden anhand des zu Grunde liegenden Protokolls (entweder RDP oder ICA) übermittelt. Genauere Angaben folgen im Kapitel 2.4.2.

Um Anwendungen für einen Mehrbenutzerbetrieb installieren zu können, muss der Server zuerst in den Installationsmodus umgestellt werden. Nach dieser Änderung können Anwendungen wie üblich installiert werden, wobei Registrierungseinträge in einem Mappingvorgang in einen systemweiten Bereich kopiert werden, um diese später beliebigen anderen Benutzern verfügbar zu machen (vgl. MO03, S.107).

Nicht alle Applikationen sind in einer Mehrbenutzer Umgebung lauffähig. Ausschlaggebend hierfür ist der Zugriff auf gemeinsam genutzte Komponenten wie DLL und INI Dateien, sowie auf die Registrierungsdatenbank. Selbst wenn eine Applikation einzeln auf dem Terminal Server lauffähig ist, kann sich das ändern, sobald eine weitere Applikation installiert wird, die vielleicht einige wichtige Einstellungen überschreibt. Eine ausführliche Beschreibung der Problematik der Applikationskonflikte und deren Lösung findet sich in Kapitel 3.1.2.

Die aktuelle Version des RDP Protokolls unterstützt eine Farbtiefe bis 24 Bit (16 Millionen Farben) und eine Auflösung bis zu 1600 * 1200 Pixel. Somit die Bildschirmausgabe des Servers farbgetreu auf dem Client zu sehen (vgl. Tri03, S.84).

Für alle Plattformen wie z.B. Linux, Macintosh usw. sind Software Clients entweder von Microsoft oder von einem anderen Anbieter verfügbar. Terminal Server können also von nahezu jedem Clientgerät benutzt werden.

Mit Hilfe des Web Clients ist mit einem Browser der Zugriff auf den Terminal Server möglich. Benutzer starten über den Browser einen Remote Desktop auf dem Terminal Server (siehe Abbildung 2.2). Der Web Client ist ein ActiveX Steuerelement,

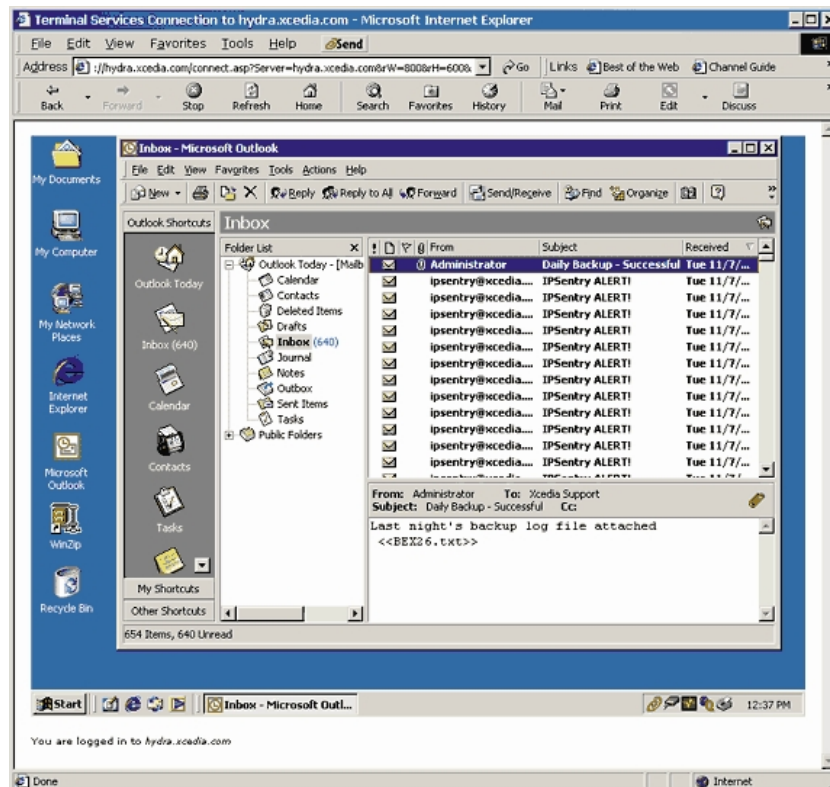


Abb. 2.2: Mit dem Web Client für Terminal Server kann der Benutzer eine Remote Desktop Umgebung im Browser starten.
Quelle: Windows IT Pro

das innerhalb einer Seite eingebaut wird und eine RDP Session mit dem Terminal Server startet (vgl. [Tri03](#), S.429).

Benutzerkonten und Gruppenrichtlinien steuern den Zugriff der Benutzer auf Applikationen und Ressourcen. Dabei kann entweder auf bereits erstellte Gruppen aus dem Active Directory der Domäne zugegriffen oder eigene Gruppen für den Terminal Server erstellt werden. Neben dem Zugang sind auch Verbindungsparameter und andere Einstellungen für die Gruppen möglich (vgl. [Tri03](#), S.152 f.).

Mit Benutzerprofilen können Einstellungen des Benutzers zur Windows Oberfläche und Konfiguration, zur Internet Verbindung, zu Druckern und Netzwerklaufwerken und zu Applikationseinstellungen gespeichert werden. Bei erneuter Anmeldung werden diese Einstellungen wieder geladen. Da sich die Benutzer von verschiedenen Rechnern aus auf den Terminal Server verbinden können, besteht die Möglichkeit, neben einem lokal auf dem Rechner vorhandenen Benutzerprofil, auch

ein Benutzerprofil auf dem Server zu laden. Somit ist gewährleistet, dass der Benutzer immer die gewünschten Einstellungen vorfindet, egal an welchem Rechner er sitzt.

Der Administrator kann Benutzerprofile auch vorgeben, um Änderungen von Einstellungen durch die Benutzer zu verhindern und damit eine bessere Kontrolle gewährleisten zu können. Da unter Umständen eine Unterscheidung getroffen werden soll, ob sich ein Benutzer auf einen "normalen" Server oder auf einen Terminal Server verbindet, gibt es die Möglichkeit neben dem normalen Server Profilpfad auch einen Terminal Services Profilpfad anzugeben (vgl. [MO03](#), S.148 f.).

Das Verwalten von Druckertreibern sind ein Teil des beim Server Based Computing schon immer bestehenden Problems des Druckens. Die Abläufe beim Drucken sind relativ komplex in einer Terminal Service Umgebung und werden hier nur kurz besprochen. Je nachdem ob es sich um einen am Client lokal verfügbaren Drucker, einen freigegebenen Netzwerkdrucker oder einen an den Terminal Server angeschlossenen Drucker handelt, muss der Druckertreiber, der das druckerunabhängige Format EMF (=Enhanced Metafile Format) in das jeweils richtige Zielformat bringt, auf dem Server oder dem Client verfügbar sein. Druckaufträge können entweder vom Server oder Client ausgehen und wiederum jeweils vom Server oder Client ausgeführt werden. Die Verteilung der Druckertreiber ist dabei kritisch und wird mit Hilfe von z.B. universellen Druckertreibern, die bei Citrix zum Einsatz kommen, vereinfacht. Trotzdem bleibt das Drucken ein Gebiet mit Verbesserungsbedarf, da das Senden der Rohdaten des Druckauftrages über das Netzwerk eine Menge Bandbreite verbraucht (vgl. [Tri03](#), S.174).

"Session Shadowing" bezeichnet die Fernsteuerung von Terminal Server Sessions (eine genauere Erklärung zu Sessions befindet sich im Kapitel [2.4.1](#)). Damit ist es einem Benutzer nach entsprechender Zustimmung möglich, die Session eines anderen Benutzers zu steuern. Einsatzgebiet ist z.B. das Help Desk, bei dem der Administrator Probleme nicht mehr lokal auf den einzelnen PCs lösen muss, sondern sich mit der betroffenen Session verbindet. Ein Trainingsszenario ist ebenfalls denkbar, bei dem ein Benutzer einem anderen Benutzer den Ablauf eines Arbeitsvorgangs demonstriert ohne vor Ort zu sein (vgl. [Mad02](#), S.648).

Terminal Server unterstützt die Verwendung der Zwischenablage zwischen Client und Server. Falls ein Benutzer eine Datei oder ein Stück Text lokal auf dem Rechner ausschneidet, kann er sie in der Serverumgebung wieder einfügen und umgekehrt.

Lokale Laufwerke können auf dem Terminal Server z.B. mit dem Windows Explorer oder auch von gestarteten Applikationen verwendet werden. Das Mapping der lokalen Laufwerke ist erst seit der Version Windows Server 2003 enthalten (vgl. [Mad02](#), S.50).

Bei Windows 2003 Server existiert ein Load Balancing Mechanismus in Form des "Network Load Balancing" (NLB). Dabei wird eine Gruppe von Servern durch eine einzige IP-Adresse repräsentiert, Verbindungsversuche werden reihum auf die Server verteilt. Benutzer werden nach dem Verlust der Verbindung beim nächsten Verbindungsaufbau wieder zum gleichen Server verbunden um die dortige Session wieder aufzunehmen. Dieses Prinzip berücksichtigt jedoch in keiner Weise die tatsächliche Belastung der Server bezüglich der CPU- oder der Hauptspeichernutzung, sondern beruht lediglich auf Daten über die Netzwerkauslastung. Außerdem kommunizieren die Server nicht miteinander, um Lastinformationen auszutauschen, und es gibt eine Begrenzung von 32 Servern, die von NLB unterstützt werden (vgl. [Dre05](#), S.43).

Die Funktionalität von Microsoft Terminal Server kann durch Anbieter von Zusatzsoftware erweitert werden. Bekannte Produkte sind neben Citrix *Presentation Server*, die ursprünglich von Tarantella entwickelte und nun von Propalms angebotene Software TSE und Cockpit von Jetro Platforms. Allerdings führen Konkurrenzprodukte im Vergleich zum marktführendem *Presentation Server* nur ein Nischendasein.

Alle diese Produkte verfügen über die vier wichtigsten Verbesserungen für Terminal Server (vgl. [Mad02](#), S.27 f.):

- Publiizierte Anwendungen (Application Publishing)
- Seamless Window
- Ausgereiftes Webinterface
- Load Balancing

Der größte Vorteil bei z.B. Citrix liegt im Zugang zu den Applikationen. Während sich beim normalen Terminal Server der Benutzer immer über einen kompletten Remote Desktop zu einer Anwendung verbindet, bietet Citrix auch die Möglichkeit, mit

Hilfe von "Application Publishing" und "Seamless Window" direkt Anwendungen auf einem beliebigen Server zu starten.

Beim Application Publishing wird einer Anwendung, die auf einem Server der Farm installiert ist, ein logischer Name zugewiesen. Startet ein Benutzer diese Anwendung, wird aufgrund des logischen Namens ein beliebiger Server gewählt, der diese Anwendung zur Verfügung stellt. Die Anwendungen werden also für die gesamte Citrix Umgebung und für eine bestimmte Gruppe von Benutzern veröffentlicht. Es erfolgt damit eine Trennung der logischen Installation der Anwendung auf der Serverfarm und der physikalischen Installation auf einem der Server (vgl. Lüd06, S.219 f.).

Seamless Window ist der Fachausdruck für die nahtlose Integration einer Terminal Server Anwendung auf einem lokalen Rechner. Der Benutzer erkennt dabei bis auf den automatischen Login Mechanismus nicht, ob er eine lokal installierte oder eine auf dem Terminal Server laufende Anwendung benutzt. Es wird nur das Applikationsfenster gezeigt, und da die Applikation nicht innerhalb eines Remote Desktops gestartet wird, sieht der Benutzer auch nicht die übliche, zusätzliche Taskleiste (vgl. Lüd06).

Es ist außerdem möglich, die Anwendungen komplett auf dem lokalen Rechner zu integrieren. Benutzer können, wie bei lokalen Installationen, Verknüpfungen auf den Desktop oder in die Startleiste legen. So kann eine Mischung aus lokalen und Terminal Server Anwendungen, wie sie in den meisten Firmen vorkommt, realisiert werden, ohne dass der Benutzer einen Unterschied merkt bzw. die Methodik oder Effizienz seiner Arbeit eingeschränkt wird.

Zum Beispiel hat eine Firma ein sehr spezialisiertes, lokal installiertes Finanzprogramm, das nur von wenigen Benutzer benutzt wird. Alle diese Benutzer verwenden zusätzlich Excel für Tabellenkalkulation, das für die ganze Firma als publizierte Anwendung auf dem Terminal Server vorliegt. Das Finanzprogramm und Excel hätten beide Einträge im Startmenü und würden sich auch sonst in ihrer Umgebung nicht voneinander unterscheiden.

Dies erleichtert zum einen das Handling für die Benutzer, da sie im besten Fall nicht einmal merken, dass die Anwendung zentral auf dem Server läuft und sie nicht von einem oder mehreren Remote Desktops verwirrt werden.

Zum anderen fördert es auch die Sicherheit, da der Zugang zu Applikationen leichter kontrolliert werden kann (vgl. [Mad02](#), S.120 f.).

Alle für einen Benutzer publizierten Anwendungen können an Hand der *Program Neighborhood* eingesehen werden. Die *Program Neighborhood* stellt alle Anwendungen mit den gewohnten Icons dar und startet sie je nach Einstellung z.B. in einem Seamless Window.

Die *Access Suite* von Citrix beinhaltet auch ein Webinterface, mit dem es möglich ist, die *Program Neighborhood* in einem Browser darzustellen. Damit ist ein Zugriff auf publizierte Anwendungen über das Internet möglich. Das Webinterface basiert auf ASP.NET und kann nach Belieben z.B. dem Corporate Design einer Firma angepasst werden und in anderen Seiten oder Portale der Firma integriert werden (vgl. [Bod05](#), S.420). Ein konkretes Beispiel zur Integration des Webinterfaces in eine Website findet sich in Kapitel 6.

Das Webinterface wird auf dem IIS (=Internet Information Services) Server von Microsoft, der im Funktionsumfang von Windows Server enthalten ist, gehostet. Per XML erhält das Webinterface Daten über die publizierten Anwendungen vom *Presentation Server* und schickt den HTML Code für die *Program Neighborhood* an den Client. Startet der Benutzer eine Anwendung, wird eine Datei vom Webinterface an den Client übermittelt, in der alle benötigten Daten zum Verbindungsaufbau auf den *Presentation Server* mittels ICA (=Independent Computing Architecture) enthalten sind (vgl. [Lüd06](#), S.352 f.).

Ein weiterer Grund, weshalb Citrix vor allem bei großen Unternehmen eine notwendige Investition darstellt, ist das Load Balancing. Beim *Presentation Server* erfolgt die Zuweisung des Benutzers zu einem physikalischen Server nach definierbaren Regeln, bei denen z.B. die Benutzerlast des Servers, die CPU-Auslastung oder die Speicherbelegung berücksichtigt werden können. Im Gegensatz zu normalen Terminal Service Umgebungen werden die Sitzungsinformationen auf dem *Presentation Server* verwaltet. Somit ist es nicht erforderlich ein Session Directory (das nicht in der Standard Edition, sondern nur in der Enterprise Edition von Windows Server enthalten ist) mit zusätzlichem Backupserver als Redundanz einzurichten (vgl. [Bod05](#), S.412).

Interessant ist zudem die Citrix *Speed Screen* Technik, die verbesserte Komprimierungsalgorithmen beim ICA Protokoll beinhaltet und für eine kleine Mogelei steht, bei der die Wahrnehmung der Anwender getäuscht wird. *Speed Screen* zeigt Tas-

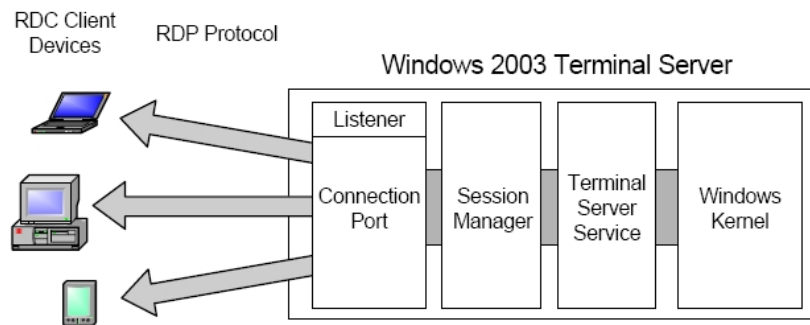


Abb. 2.3: Die Komponenten des Terminal Servers. Quelle: (MO03)

atureingaben direkt am Bildschirm an, schon bevor sie der Server verarbeitet und zurück an den Client schickt. Dieses Feature ist besonders im WAN-Umfeld wirkungsvoll, da Anwender sofort am Bildschirm die eingegebenen Daten sehen. Es reduziert den Netzverkehr und erhöht zusätzlich die Reaktionsfähigkeit des Systems (vgl. Wes04).

2.4 Technische Funktionsweise

Die Funktionalität von Terminal Services umfasst das für den Mehrbenutzer Betrieb fähige Betriebssystem und das zwischen Serverdienst und Clientsoftware verwendete Präsentationsprotokoll (RDP oder ICA). Darüber hinaus ist eine Anbindung zusätzlicher Netzwerkkomponenten für den Betrieb nötig. In den nächsten Kapiteln wird die technische Funktionsweise dieser Bestandteile für Terminal Services genauer erklärt.

2.4.1 Mehrbenutzer Betriebssystem

Der Terminal Server ist im Grunde genommen dasselbe wie ein normaler Windows Server, nur dass bestimmte Komponenten hinzugefügt wurden, um mehrere gleichzeitig agierende Benutzer zu unterstützen (siehe Abbildung 2.3). Unter Mehrbenutzerfähigkeit kann man sich dabei die Bereitstellung von mehreren Desktop Interfaces vorstellen. Die Benutzer bedienen gleichzeitig je eine "Remote Desktop" Umgebung, die vom Terminal Server zur Verfügung gestellt wird, und können jeweils völlig unterschiedliche Aufgaben erledigen.

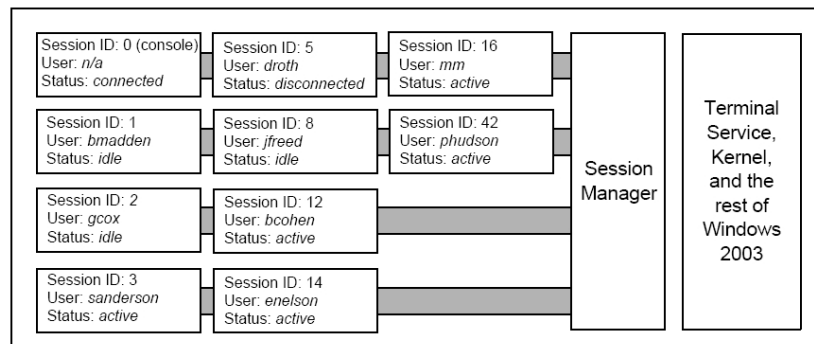


Abb. 2.4: Der Session Manager verwaltet die aktuellen Verbindungen zum Terminal Server. Quelle: (MO03)

Um das Betriebssystem und die Benutzer untereinander zu schützen, laufen alle verwendeten Anwendungen im Benutzermodus. Gemeinsam benutzte Betriebssystemprozesse könnten aber immer noch zu Konflikten und Abstürzen führen. Deswegen teilt der Terminal Server Ressourcen konsequent in Sessions ein (vgl. MO03, S.36).

Dafür wird zum einen der Speicherbereich des Betriebssystems für Prozesse, die kritisch im Mehrbenutzer Betrieb sind, in den virtuellen Speicher kopiert. Zum anderen wird der Terminal Services Dienst (*termserve.dll*), der u.a. den Session Manager startet, beim Start des Betriebssystems geladen. Der Session Manager verwaltet und überwacht alle Benutzer Sessions.

Jedes Mal, wenn ein Benutzer sich mit dem Server verbindet und ihm ein Remote Desktop zur Verfügung gestellt wird, erzeugt der Server eine Session ID zur Unterscheidung der Benutzer (siehe Abbildung 2.4). Mit Hilfe der Session ID wird z.B. auch die Speicherzuweisung verwaltet. Wenn sich der Benutzer ausloggt, wird der ihm zugeordnete Bereich im Speicher gelöscht.

Da bei den Sessions Speicher und Prozesse getrennt gehalten werden, sollten Fehler, von z.B. Applikationen in einer Session, die anderen Sessions nicht beeinflussen. In Wirklichkeit laufen die Sessions immer noch auf dem gleichen Server und benutzen zum Teil die gleichen Ressourcen. Wenn eine Session einen Bluescreen des Servers und damit einen Stillstand des Betriebssystems bewirkt, hat das natürlich auch Auswirkung auf die anderen Sessions (vgl. MO03, S.37). Ein gutes Beispiel dafür sind z.B. viele Druckertreiber, die immer im exekutiven Teil des Betriebssys-

tems laufen. Ein Absturz des Systems beim Druckauftrag bewirkt den Stop des kompletten Terminal Servers (vgl. [Tri03](#), S.174).

Die Sessions werden mit Hilfe des RDP Protokolls, das im nächsten Abschnitt genauer betrachtet wird, gesteuert. Die Benutzer verbinden sich mit einem RDP fähigen Client an einen der Ports des Servers. Der Server kann mehrere Netzwerkkarten enthalten und weist jeder einen eigenen Port zu. Jeder Port hat eine Listener Komponente, die kommende Requests annimmt und an den Session Manager weiterleitet.

Zusatzsoftware wie der Citrix *Presentation Server* nutzen die vorgegebenen Eigenschaften des Terminal Servers und bestehen im Grunde genommen aus zusätzlichen Diensten und Managementwerkzeugen, die das Sessionmanagement, die Lizenzierung, das Verwalten von Anwendungen und den Lastenausgleich zwischen den Servern übernehmen. Der zu Grunde liegende Terminal Server wird dabei nicht verändert, und so ist es auch möglich, dass sich theoretisch gleichzeitig Benutzer mit RDP am Terminal Server und Benutzer mit dem ICA Protokoll am *Presentation Server* anmelden.

2.4.2 Präsentationsprotokoll

Im ersten Teil wird auf das RDP von Microsoft, das beim normalen Terminal Server zum Einsatz kommt, eingegangen, anschließend wird das ICA Protokoll von Citrix für den *Presentation Server* vorgestellt.

Das RDP Protokoll erlaubt die Kommunikation zwischen Server und Client mit bis zu 64.000 virtuellen Kanälen. Dabei werden Bildschirminhalte vom Server als Bitmap bzw. Rastergrafik zum Client übertragen. Der Client übermittelt Maus- und Tastaturinteraktionen zum Server. Die Kommunikation verläuft dabei asymmetrisch, wobei der deutlich größere Teil der Daten vom Server an den Client geschickt wird (vgl. [MO03](#), S.25).

RDP basiert auf dem TCP/IP Protokoll und enthält mehrere Schichten. Die unterste Ebene ist zuständig für den Verbindungsaufbau, die Verbindungsbestätigung und den Verbindungsabbau zwischen Client und Server. Darüber liegt eine Schicht für Multicastdienste, die eine Punkt-zu-Mehrpunkt Verbindung z.B. für die Remoteüberwachung einer Session durch einen anderen Benutzer erlaubt. Eine Sicherheitsschicht umfasst alle Dienste im Hinblick auf Verschlüsselung und Signatur.

Damit die RDP Verbindung nicht abgehört oder modifiziert werden kann, wird

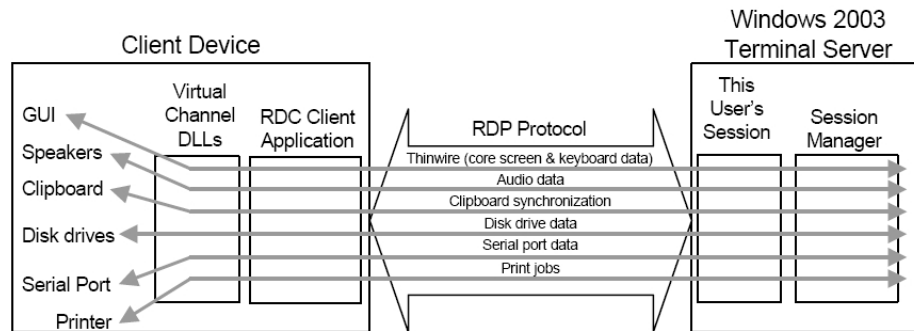


Abb. 2.5: Mit Hilfe von virtuellen Kanälen lassen sich Daten in einer RDP Sitzung austauschen. Quelle: (MO03)

der Datenstrom mit dem RC4 Algorithmus verschlüsselt, sowie eine Signatur mit Hilfe von MD5 und SHA-1 erstellt. Die relevante Schicht des Protokolls liegt darüber und ist für die eigentliche Übertragung der Bildschirmausgaben bzw. Tastatureingaben zuständig. Der Mechanismus ist recht aufwändig und umfasst z.B. das Aushandeln von Verbindungsparametern und das Cachen (bzw. Zwischenspeichern) gewisser Daten zur Reduktion der Netzlast (vgl. Tri03, S.80).

RDP verwendet sogenannte virtuelle Kanäle zur Übertragung zusätzlicher Daten zwischen Client und Server.

Darunter fallen (siehe Abbildung 2.5):

- Audiodaten, die vom Server auf den Client übertragen und dort abgespielt werden
- Lokale Laufwerke auf dem Client, die auf dem Server benutzt werden können
- Lokale Drucker, die in der Terminal Service Umgebung nutzbar sind
- Serielle Ports für am Client verbundene Geräte
- Die Windows Zwischenablage

Ein virtueller Kanal besteht aus einer Server- und einer Clientkomponente. Auf dem Server wird ein Dienst für die Session des Benutzers gestartet, während auf dem Client meistens eine DLL Datei beim Start der RDP Software geladen wird. Es ist auch

möglich eigene virtuelle Kanäle zu definieren und zu benutzen. Die meisten Add-on Produkte für Terminal Server nutzen diese Möglichkeit (vgl. [MO03](#), S.40 f.).

Durch das RDP Protokoll werden auch Optionen für die Verbindung ausgehandelt, je nachdem, mit welcher Art von Client man Kontakt aufnehmen möchte. Anhand von Informationen zu Hardware, Betriebssystem, Protokollversion und unterstützte Datenkompression des Client wird festgelegt:

- Größe des Desktop
- Unterstützte Farbanzahl und -tiefe
- Cachingmethode
- Stärke der Kompression

Durch die ausgereifte Kompression der Bilddaten und dem Caching wird der Bandbreitenbedarf auf durchschnittlich 15 kBit/s pro Session stark reduziert (vgl. [Tri03](#), S.81 f.).

Das ICA Protokoll von Citrix, das früher dem RDP Protokoll in vielen Punkten wie z.B. Geschwindigkeit überlegen war, ist inzwischen vergleichbar mit der aktuellen Version von RDP. Beim ICA Protokoll werden ebenfalls virtuelle Kanäle zur Steuerung der Datenübertragung genutzt und es unterstützt damit die gleichen Funktionalitäten wie bereits oben beschrieben.

Die wesentlichen Vorteile des ICA Protokolls gegenüber RDP sind:

- Der "Session Reliability", also dem automatischen Wiederaufbau der Verbindung zum Server nach einem Verlust der Netzwerkverbindung (besonders nützlich z.B. bei Benutzern mit instabiler Wireless Verbindung) (vgl. [Dre05](#), S.110)
- Der *Speed Screen* Funktionalität (vgl. Kapitel [2.3](#))
- Der Möglichkeit ICA Pakete neben TCP/IP auch über IPX, SPX, NetBios und SSL zu übertragen (vgl. [Mad02](#), S.355)

Gerade das Senden von ICA Paketen durch einen SSL Tunnel bringt viele Vorteile und wird in Kapitel [3.4](#) genauer erläutert. Die "Smooth Roaming" Funktion, die im Rahmen des Mobile Computing in Kapitel [2.6.2](#) angesprochen wird, ermöglicht

einen problemlosen Wechsel zwischen unterschiedlichen Endgeräten innerhalb einer aktiven Sitzung.

Zusammen mit der großen Auswahl an Clientsoftware bietet Citrix damit eine umfassende Unterstützung aller möglichen Systeme und Netzwerke. Neben mehreren Windows Clients, die sich in ihrem Umfang (z.B. *Program Neighborhood Client* und *Program Neighborhood Agent*) und ihrer Funktionalität (z.B. Webclient für den Browser) unterscheiden, gibt es auch einen plattformunabhängigen Java Client. Damit ist es z.B. möglich mit einem Clientgerät auf dem Linux installiert ist, Windows Applikationen auf dem Terminal Server zu starten.

2.4.3 Netzwerkachitektur

In diesem Kapitel wird näher auf die Netzwerkachitektur eingegangen und wie diese aufzubauen ist, um bestimmte Ziele zu erreichen. Die beiden wesentlichen Punkte sind dabei (vgl. MO03, S.52):

- Der Standort bzw. die Standorte von Terminal Servern
- Standorte der benötigten, unterstützenden Server

Die Standortwahl der Server ist deshalb so wichtig, weil sie direkten Einfluss auf Geschwindigkeit und Qualität der Benutzer Session hat, den Bandbreitenbedarf beeinflusst und die Komplexität des Server Managements bestimmt (vgl. MO03, S.55).

Die empfundene Geschwindigkeit einer Session hat dabei nicht nur mit der Bandbreite zwischen Server und Client zu tun, sondern auch mit der Anbindung von Datenquellen an den Terminal Server. Der verursachte Datenverkehr einer Applikation ist, mit wenigen Ausnahmen, meistens sehr viel höher als der entstehende RDP Traffic einer Terminal Server Session. Für die Verwaltung der Server ist zu entscheiden, ob die Server und die Applikationen am gleichen Standort administriert werden müssen (vgl. MO03, S.56).

Es gibt zwei unterschiedliche Ansätze für den Aufbau einer Terminal Server Architektur. Beim zentralen Ansatz wird die Terminal Server Farm für alle Benutzer Standorte in einem Rechenzentrum aufgebaut (siehe Abbildung 2.6). Dadurch kann die Farm leicht betrieben und verwaltet werden. Die Benutzer haben über einen Server Zugang zu all ihren Applikationen. Falls allerdings auf Datenquellen, die sich an

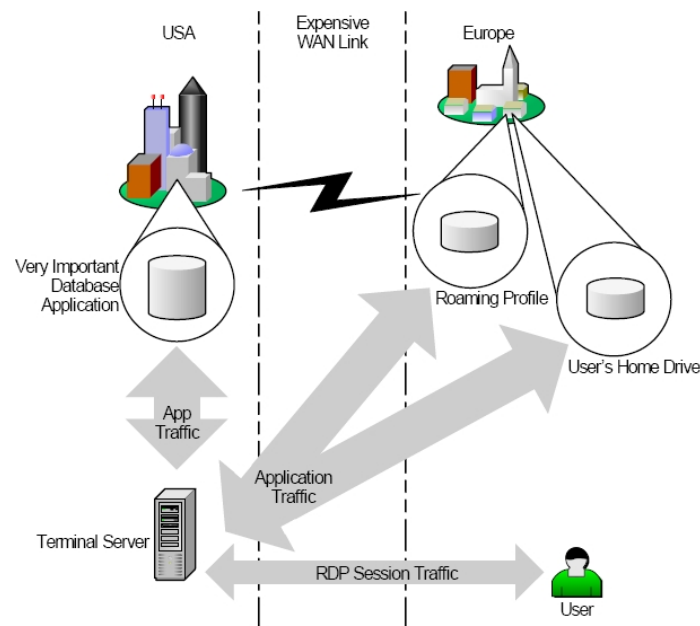


Abb. 2.6: Bei einer zentralen Architektur wird die Bandbreite mit der Datenübertragung belastet. Quelle: (MO03)

anderen Standorten befinden, zugegriffen wird, kann die Geschwindigkeit der Session erheblich leiden. Die Ausfallsicherheit einer zentralen Lösung ist nicht gegeben, da entweder die Serverfarm oder die Verbindung zwischen den Standorten ausfallen kann (vgl. MO03, S.58 f.).

Beim dezentralen Ansatz werden für mehrere Standorte Terminal Server eingerichtet. Die Applikationen werden auf Grund der benötigten Datenanbindung vorteilhaft auf die verschiedenen Server verteilt. Damit haben die Benutzer schnellen Zugriff auf ihre Daten und die WAN Bandbreite wird effektiv genutzt (siehe Abbildung 2.7). Falls ein Server ausfällt, können immer noch die Applikationen auf dem anderen Server benutzt werden. Dafür wird die Architektur komplexer und Benutzer müssen sich zu mehreren Servern verbinden, um Zugang zu allen erforderlichen Applikationen zu erhalten. Außerdem ist die Administration komplizierter, da jeder Standort einzeln verwaltet werden muss (vgl. MO03, S.56 f.).

Um eine Entscheidung für eine der Optionen zu treffen, muss vorher in Betracht gezogen werden, wo sich die Benutzer befinden. Sind sie auf mehrere Standorte verteilt, ist das Zahlenverhältnis der Benutzer entscheidend. Der wichtigste zu analysierende Punkt ist, wo sich die Datenquellen befinden, die ein Benutzer bei der Arbeit

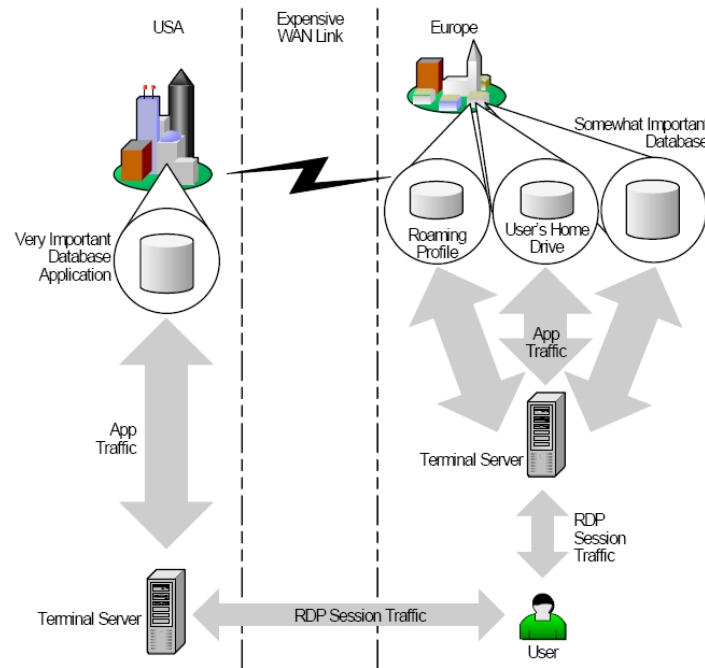


Abb. 2.7: Bei einer dezentralen Architektur läuft nur das Präsentationsprotokoll über das WAN. Quelle: (MO03)

mit einer Anwendung benötigt. Besonders die Häufigkeit und der Umfang des Zugriffs sind dabei von Bedeutung. Es spielt eine Rolle, wie viele Applikationen auf den einzelnen Terminal Servern zur Verfügung gestellt werden sollen, und es muss für jede Anwendung die Entscheidung getroffen werden, ob sie auf dem Terminal Server oder besser lokal betrieben werden sollte. Zwei weitere Punkte, die zur Entscheidung beitragen, sind, wie die Unterstützung der IT Abteilung für die einzelnen Anwendungen geregelt ist, bzw. ob die Administratoren vor Ort sein müssen, und wie hoch die Bandbreite und die Zuverlässigkeit der WAN Verbindung ist (vgl. MO03, S.60 f.).

Der Terminal Server braucht für den Betrieb zwei unterstützende Server: das Session Directory und den Lizenzserver (siehe Abbildung 2.8). Von beiden wird im laufenden Betrieb ausgiebig Gebrauch gemacht, weshalb es sich anbietet, pro Standort eines Terminal Servers ein Session Directory und einen Lizenzserver anzubinden (vgl. MO03, S.64 f.).

Für den Citrix *Presentation Server* gelten alle oben angeführten Überlegungen, bis auf das Session Directory. Da der *Presentation Server* die Sessions selbst verwaltet, ist ein extra Session Directory unnötig.

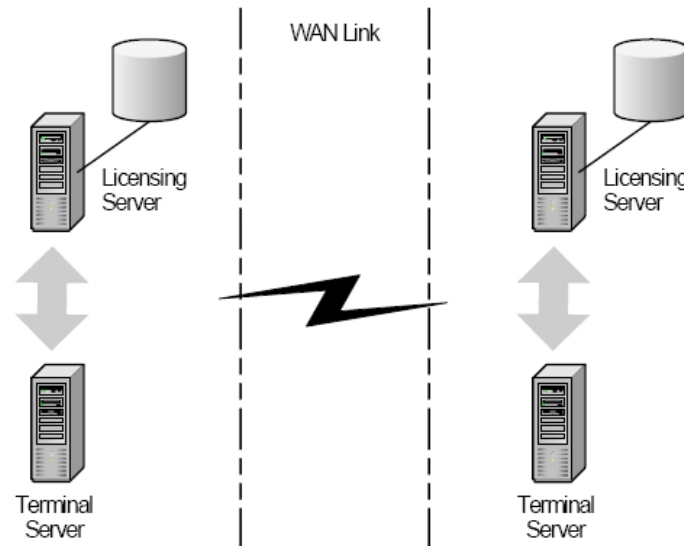


Abb. 2.8: Jedem Terminal Server sollte ein Lizenzserver zugeordnet sein um einen schnellen Zugriff zu gewährleisten. Quelle: (MO03)

2.5 Vergleich der Terminal Services mit anderen Architekturen

Die Entscheidung für Terminal Services geht einher mit einer nachhaltigen IT Strategie für das Unternehmen. Ob Terminal Services oder ein klassisches Netzwerk mit PCs für ein Unternehmen sinnvoll ist, entscheidet letztendlich die Gewichtung der Vor- und Nachteile der Lösungen, die hier aufgelistet werden.

2.5.1 Vor- und Nachteile der Terminal Services

Die Funktionalität der Terminal Services wurde bereits im Kapitel 2.3 besprochen. Die daraus resultierenden Vorteile sind (vgl. Bod05, S.404):

- Einfacher, zentraler Betrieb und Verwaltung von Applikationen
- Einsparung von Lizenzkosten bei den verwendeten Applikationen, da die Benutzer nur die Applikationen nutzen, die sie wirklich benötigen
- Weniger Zeit und damit Kosten für die Wartung der Client Rechner und Einsparungen beim HelpDesk (siehe Abbildung 2.9)

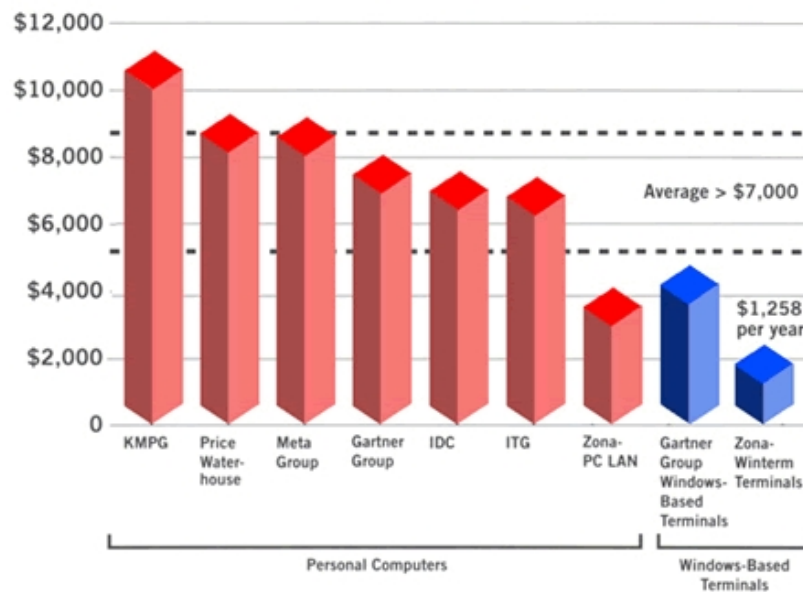


Abb. 2.9: Studien belegen anhand der TCO die Einsparungen bei der Nutzung von Terminal Services anstatt traditioneller PCs.
Quelle: ETCF

- Applikationen können von überall und mit jedem Clientgerät genutzt werden (bei einem Einsatz von Citrix)
- Hohe Flexibilität bei der Erweiterung und Änderung der IT Infrastruktur
- Hoher Sicherheitsstandard, da Applikationen und Daten nicht das Firmennetzwerk verlassen

Die Terminal Services bringen jedoch auch folgende Nachteile (vgl. [Bod05](#), S.405):

- Hohe Erstanschaffungskosten für eine leistungsfähige Serverfarm
- Einige Applikationen sind nicht lauffähig in einer Mehrbenutzer Umgebung
- Applikationskonflikte sind bei einer großen Zahl von installierten Applikationen sehr wahrscheinlich, da jede Applikation ihre Spuren wie Registrierungseinträge oder DLL Dateien im Betriebssystem hinterlässt
- Einschränkung der Freiheit der Benutzer und damit unter Umständen Einbußen bei der Effizienz

- Kein Offlinebetrieb der Applikationen möglich
- Mangelnde Ausfallsicherheit bei einer zentralen Architektur, da der Terminal Server ein "single point of failure" darstellt bzw. es besteht ein Bedarf an Redundanz, der sehr kostenintensiv sein kann

2.5.2 Vor- und Nachteile Personal Computers

Ein übliches Szenario in einem Unternehmen könnte so aussehen, dass jeder Benutzer seinen eigenen PC besitzt. Auf diesem PC sind alle Applikationen die er benötigt installiert und entweder seine ganzen Daten oder ein Teil seiner Daten (neben z.B. Netzwerklaufwerken) gespeichert.

Je nachdem, ob der Benutzer volle Administrationsrechte oder eingeschränkte lokale Rechte auf dem Rechner besitzt, kann er Einstellungen des Systems ändern und neue Anwendungen installieren.

Üblicherweise sind die PCs der einzelnen Mitarbeiter in einem Netzwerk verbunden, was es möglich macht Dateien auszutauschen und z.B. einen gemeinsamen Internetzugang zu nutzen. Ohne den Einsatz von Zusatzsoftware, wie im nächsten Kapitel 2.5.3 beschrieben, muss Anwendersoftware auf jedem Rechner mit einer Installations-CD oder über ein Netzwerklaufwerk manuell installiert werden.

Der Einsatz von Personal Computer hat folgende Vorteile (vgl. Mad02, S.349):

- Der Benutzer hat ein großes Maß an Freiheit und kann seine Arbeitsumgebung komplett seinen Bedürfnissen anpassen
- Die Rechenleistung wird über mehrere Systeme verteilt und rechenintensive Anwendungen können problemlos lokal ausgeführt werden
- Der Benutzer kann auch bei einem Netzwerk- oder Serverausfall lokal weiterarbeiten
- PCs sind nahezu für alle möglichen Arbeitsprozesse universell einsetzbar
- Auch Applikationen die nicht mit Terminal Services lauffähig sind, können benutzt werden
- Die Benutzer sind an diese Art der Arbeit gewöhnt

Dem stehen allerdings auch zahlreiche, z.T. gravierende Nachteile gegenüber (vgl. [Mad02](#), S.349):

- Der Wartungsaufwand ist enorm, da Probleme an vielen unterschiedlichen Rechnern auftreten können und behoben werden müssen
- Installationen müssen auf jedem Rechner manuell durchgeführt werden und es wird jeweils eine Benutzerlizenz für jede Installation benötigt
- Anwendungen innerhalb eines Unternehmens können unterschiedliche Versionen haben
- Es gibt keinen einheitlichen Zustand der Rechner, da die Benutzer unterschiedliche Einstellungen vornehmen können und es somit verschiedene Kombinationen von Software und Hardware gibt
- Die PCs müssen nach einer kurzen Zeitspanne erneuert werden, um mit den erhöhten Rechenanforderungen von Applikationen Schritt zu halten

2.5.3 Vor- und Nachteile automatische Softwaredistribution

Um die Wartungskosten für PCs zu reduzieren, besteht die Möglichkeit einer Art Zwischenlösung mit einer automatischen Softwaredistribution. Hierbei müssen die Benutzer oder der Administrator die Anwendungen bzw. benötigte Updates und Patches für bestehende Anwendungen nicht mehr manuell auf jedem Rechner einzeln installieren, sondern die Anwendungen werden von einem zentralen Server aus über das Netzwerk an die Client Rechner verteilt.

Für das automatische Verteilen von Software in einem Netzwerk gibt es mehrere Anbieter. Hier wird näher auf das Produkt SMS (=Systems Management Server) von Microsoft eingegangen.

Zusätzlich zu der automatischen Verteilung von Software erfragt und sammelt SMS Daten über die einzelnen Rechner im Netzwerk (z.B. welches Betriebssystem und welche Hardware besitzt der Rechner) und erleichtert damit die Fehlersuche.

Beim SMS muss für jede Applikation eine Installationsroutine in Form einer MSI (=Microsoft Installer) Datei auf dem Server erstellt werden. Ein MSI Paket ist ein standardisiertes, selbstablaufendes Installationspaket. Diese MSI Datei wird dann Gruppen von Rechnern zugeordnet (vgl. [Tre03](#)).

Die Client PCs erhalten einen SMS Agenten, der prüft, welche Anwendungen bereits installiert sind und welche vom SMS für den Rechner angeboten werden. Je nach Einstellung installiert sich eine neue Anwendung automatisch oder der Benutzer stimmt der Installation auf dem Rechner explizit zu. Alle Anwendungen, die dem Benutzer zur Verfügung stehen, können als "Advertised Programs" eingesehen werden.

Der Einsatz von SMS bietet folgende Vorteile (vgl. [Tre03](#)):

- Die Installation von Anwendungen läuft automatisch auf den Client Rechnern
- Der Administrator hat eine verbesserte Versionskontrolle und kann Updates für Anwendungen leichter verteilen
- Rechnerdetails können von zentraler Stelle eingesehen und so die Fehlersuche erleichtert werden
- Anwendungen können mit Administrationsrechten installiert werden, selbst wenn der Benutzer nur eingeschränkte lokale Rechte besitzt

Zwar erleichtert der SMS das Arbeiten in großen Netzwerken, doch gibt es auch Nachteile (vgl. [Sof06a](#)):

- Das Erstellen von MSI Installationsroutinen ist aufwändig
- Es können immer noch Software- und Hardware Konflikte auf den Client Rechnern auftreten, die an jedem PC einzeln gelöst werden müssen
- Um unterschiedliche Einstellungen bei der Installation zu unterstützen, müssen mehrere MSI Pakete erstellt werden
- Es entstehen Kosten für die Anschaffung, Inbetriebnahme und Wartung der SMS Software

Automatische Softwaredistribution löst also das Problem der Verteilung von Anwendungen, nicht aber das allgemeine Problem, dass Anwendungen auf jedem einzelnen Rechner installiert werden müssen. Es kann auch weiterhin zu Konflikten beim Zusammenspiel des Client Betriebssystems, der Hardware und mehrerer Applikationen kommen. Lösungen für diese Problematiken stellen Applikationsvirtualisierung (vgl. Kapitel [3.1.2](#)) und Streaming (vgl. Kapitel [3.3](#)) dar, die später besprochen werden.

2.6 Anwendungsszenarien für Terminal Server

Aus den gerade beschriebenen Vor- und Nachteilen von Terminal Services ergeben sich bestimmte Einsatzgebiete, für die eine Terminal Server Architektur in Unternehmen denkbar ist.

2.6.1 Thin Clients

Wird der Gedanke, der hinter Terminal Services steht, dass Applikationen auf dem Server installiert sind und dort laufen, konsequent zu Ende gedacht, kommt man zwangsläufig auf das Konzept der Thin Clients.

Der Client Rechner benötigt keine große Rechenleistung mehr und wird eigentlich nur noch als Anzeigegerät verwendet. Der Rechner braucht weder einen guten Prozessor oder viel Hauptspeicher, noch eine große Festplatte. Eigentlich sind sogar die meisten Funktionen des Betriebssystems unnötig. Das Einzige, was auf dem Clientgerät laufen muss, ist die Clientsoftware für Terminal Services. Dies kann entweder die normal installierte Software sein oder ein Browser mit einem Webclient (vgl. [KH01](#), S.284 f.).

Anbieter wie Wyse (vgl. [Wys06](#)) oder Igel (vgl. [Ige06](#)) setzen genau an diesem Punkt an. Sie bieten bis auf die absolute Basisfunktionalität reduzierte Client Rechner, mit denen man sich zum Server verbindet. Zum einen sind diese Thin Clients natürlich viel kostengünstiger als ein normaler Desktop PC, zum anderen können diese Clientgeräte viel länger genutzt werden, da es keinen wachsenden Ressourcenbedarf und damit keinen Grund für einen Austausch gibt.

Die Wartungskosten können signifikant reduziert werden, da sowohl die Applikationen und Daten zentral verwaltet werden als auch die Thin Clients durch ihre geringe Funktionalität viel stabiler laufen als herkömmliche Desktop PCs. Laut Wyse sind Thin Clients bis zu neun Mal zuverlässiger als normale PCs (vgl. [MO03](#), S.309 f.).

Der Punkt der Ausfallsicherheit hat zwei Seiten. Zwar können kaputte Thin Clients sehr leicht ausgewechselt werden, doch bedeutet ein Ausfall des Servers oder des Netzwerks das komplette Erliegen der Arbeit. Der Administrator hat deshalb für genügend Redundanz in der Serverfarm zu sorgen.

Gleichzeitig ist diese Art von Lösung eine der besten Sicherheitsentscheidungen für ein Unternehmen. Bei der höchsten Sicherheitsstufe haben die Rechner weder ein Disketten- oder CD-ROM-Laufwerk, noch einen USB Anschluss. Für die Benutzer gibt es somit keine Möglichkeit Firmendaten zu entwenden oder schädliche Software wie Viren, Würmer usw. in das Firmennetzwerk einzuschleifen. Natürlich sind auch Abstufungen bei der Sicherheit möglich (vgl. [Web06](#)).

Vorteil dieser Lösung ist neben dem Mobile Computing (siehe Kapitel [2.6.2](#)) auch die Aufhebung der traditionellen Zuweisung zwischen Computer und Benutzer. Jeder Benutzer kann im Unternehmen jeden Thin Client benutzen und trotzdem seine personalisierte und angepasste Umgebung vorfinden.

Eine Entscheidung für Thin Clients muss aber nicht immer die Richtige sein. Werden im Unternehmen regelmäßig sehr rechenintensive Applikationen verwendet, ist die Aufteilung von Rechenleistung auf mehrere Client PCs der Bündelung von Rechenleistung auf einem zentralen Server vorzuziehen. Die Sicherstellung der Performance des Terminal Servers bei gleichzeitigem Zugriff auf rechenintensive Prozesse kann sehr kostenintensiv werden.

Außerdem ist eine Entscheidung für Thin Clients auch immer eine Grundsatzentscheidung für den Umgang mit den Benutzern. Sie legt fest, welche Freiheiten den Benutzern eingeräumt werden und welches Vertrauen ihnen entgegen gebracht wird. So sollte diese grundsätzliche Entscheidung auch im Einklang mit normativen Vorgaben im Unternehmen stehen. Es ist ratsam sich schon vorher mit den Konsequenzen für die Motivation der Mitarbeiter und für das Arbeitsklima auseinander zu setzen (vgl. [MO03](#), S.310).

2.6.2 Remote und Mobile Computing

Viele Unternehmen bewegt die Frage wie benötigte Applikationen, bei Bedarf, über jede Verbindung und mit jedem Clientgerät für die Mitarbeiter zugänglich gemacht werden können. Terminal Services ermöglichen den Zugang von anderen Standorten oder von unterwegs.

Dabei sind zum einen verteilte Firmen-Standorte gemeint. Anstatt für jeden Standort eines Unternehmens Applikationen an die Clients durch eine Installation oder per automatischer Distribution zu verteilen, bleiben die Applikationen alle auf dem Terminal Server des Hauptsitzes der Firma. Die anderen Standorte sind mit dem

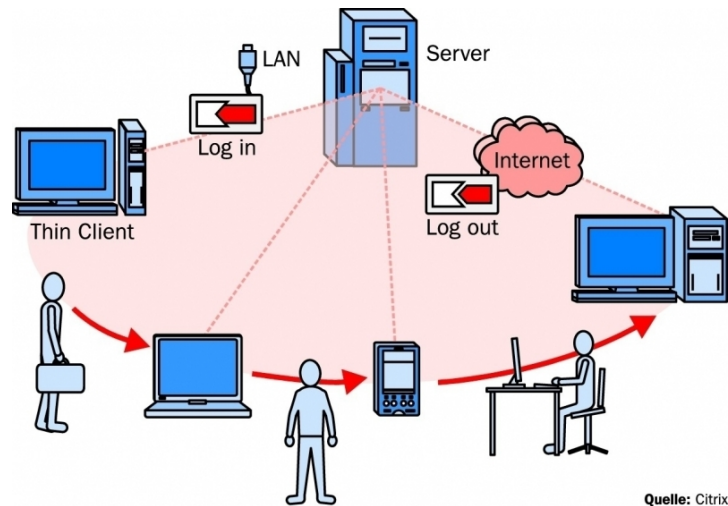


Abb. 2.10: Mit Smooth Roaming können Benutzer zwischen verschiedenen Endgeräten wechseln, ohne ihre Session beenden zu müssen. Quelle: Citrix

Hauptsitz z.B. durch ein VPN verbunden und öffnen die benötigten Applikationen dort remote auf dem Terminal Server.

Dadurch benötigt eine Firma im besten Fall nur ein zentrales Datenzentrum, spart Wartungskosten und benötigt weniger Administratoren. Voraussetzung ist allerdings eine passabel schnelle WAN Verbindung der Standorte, um einen performanten Zugang zu den Applikationen zu gewährleisten. Ein Nachteil dieser Lösung ist die mangelnde Ausfallsicherheit, wenn alle Ressourcen an einem Standort gebündelt werden.

Ein weiterer, wichtiger Fall für Firmen, die viele Mitarbeiter auf Reisen oder an sehr vielen unterschiedlichen Orten beschäftigt, ist das Mobile Computing. Durch Terminal Services können die Applikationen des Unternehmens weltweit über das Internet zugänglich gemacht werden. In Hotels, Flughäfen oder an beliebigen Standorten mit einem normalen Internetzugang, haben die Mitarbeiter vollen Zugriff auf ihren Desktop und ihre Applikationen.

Mit Hilfe des Webinterfaces benötigt der Client Rechner nicht einmal mehr einen installierten Software Client. Selbst in jedem Internetcafe, in dem ActiveX aktiviert ist, kann man sich mit einem Webbrowser zu seinen Applikationen verbinden.

Durch die Eigenschaft von Terminal Services, dass Applikationen auf dem Server ausgeführt werden, können selbst auf ressourcenarmen Clientgeräten hardwarein-

tensive Applikationen laufen. Ein bedeutendes Einsatzgebiet für Terminal Services sind damit auch PDAs, Handhelds und Handys (vgl. [Lie06](#)).

Zusätzlich bietet z.B. Citrix das Smooth Roaming, das es dem Benutzer ermöglicht, seine Session und damit alle seine Einstellungen von einem Gerät zum Nächsten zu transferieren (siehe Abbildung [2.10](#)). Dabei wird automatisch z.B. die Bildschirmauflösung und die Übertragungsrate an das Clientgerät angepasst. Eine auf dem Desktop begonnene Arbeit kann damit ganz einfach auf ein mobiles Gerät übertragen werden und der Benutzer kann weiterarbeiten, ohne seine Applikationen zu schließen (vgl. [Lie06](#)).

2.6.3 Application Service Providing

Eine der Hauptaufgaben von Terminal Services ist die Bereitstellung von Applikationen. Wie im vorangegangenen Kapitel besprochen, kann der Zugang über nahezu jede Verbindung und mit jedem Clientgerät erfolgen. Damit sind Terminal Services neben Web Services eine mögliche technische Umsetzung der Geschäftsidee des Application Service Providing.

Beim Application Service Providing werden durch einen Dienstleister Anwendungen über ein öffentliches Netz, meistens gegen Bezahlung, zur Benutzung angeboten. Damit ist es möglich Software bei Bedarf zur Nutzung anzumieten.

Der Application Service Provider ist verantwortlich für Betrieb, Bereitstellung, Management, Update und Pflege der Anwendungen und Daten. Der Kunde spart Zeit, Ressourcen und Personal und hat eine größere Flexibilität bei der Auswahl von Angeboten, sowie beim Hinzufügen und Entfernen von angemieteten Applikationen.

Natürlich schafft der Kunde damit auch eine große Abhängigkeit von der Ausfallsicherheit und Dienstqualität des Anbieters. Das Risiko kann aber durch den Abschluss von Qualitätsvereinbarungen, so genannten Service Level Agreements, kalkulierbarer gemacht werden (vgl. [KH01](#), S.35-36).

Durch Einsatz z.B. des Citrix Webinterfaces, können auch sehr komplexe und rechenintensive Anwendungen über das Internet Kunden bereitgestellt werden. Terminal Services bieten also den Application Service Providern eine günstige und verlässliche Architektur, um ihren Kunden die gewünschten Anwendungen anzubieten. Besonders bei bereits existierenden Windows Anwendungen, die mit sehr geringem

Aufwand in die Terminal Server Umgebung überführt werden können, macht eine Entscheidung für Terminal Services Sinn, da keine Anwendung neu als Web Service entwickelt werden muss.

Das Geschäftsmodell des Application Service Providing erlebt im Moment eine Renaissance, wie der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) berichtet. Nach einem ersten Boom um die Jahrtausendwende entscheiden sich viele Unternehmen wieder Mietsoftware einzusetzen. "Sie erkennen, dass sich heute dank Online-Anbindungen und intelligenter ASP-Anwendungen wirtschaftlich attraktive Lösungen realisieren lassen. Unternehmen können sich wieder stärker auf ihre Kernkompetenzen konzentrieren und so ihre Wettbewerbsfähigkeit steigern", sagt Dr. Axel Garbers (BITKOM) (vgl. [BIT06](#)).

Es muss allerdings nicht immer ein Mietverhältnis zwischen dem Anbieter von Applikationen und den Nutzern bestehen. Denkbar wäre auch eine, wie im praktischen Teil der Arbeit vorgestellt und bei Linde vorzufindende Situation, dass Tochter- oder Partnerfirmen Zugang zu Applikationen des Unternehmens erhalten. Wie in Kapitel 6 beschrieben, soll es möglich sein, Tochter- und Partnerfirmen wissenskritische Inhalte verfügbar zu machen, ohne dass die Anwendungen außer Haus gegeben werden. Mit der eingesetzten Citrix Lösung wird sicher gestellt, dass das Know How geschützt bleibt, die Benutzung von Anwendungen kontrolliert wird und die Verbreitung an nicht autorisierte Personen verhindert wird.

Kapitel 3

Entwicklungen im Bereich des Server Based Computing

Neben den Weiterentwicklungen für Terminal Services, vor allem durch Microsoft und Citrix, haben auch andere Firmen mit neuen Konzepten und Technologien Einfluss auf die Branche des Server Based Computing.

Eine Schwäche der großen Serverfarmen, die für Terminal Services in mittleren und großen Unternehmen aufgebaut werden müssen, ist die mangelnde Skalierbarkeit der Serverressourcen. Virtualisierung (siehe das nächste Kapitel 3.1) und Blades (siehe Kapitel 3.2) sind zwei relativ neue Konzepte, mit denen die Auslastung und Skalierbarkeit von Systemen verbessert werden kann. Gleichzeitig stellen beide Konzepte in bestimmten Fällen aber auch eine Alternative zu den Terminal Services dar.

Wirkliche Innovationen bietet die Firma Softricity mit ihrer *Softgrid* Plattform, die z.B. das große Problem der Applikationskonflikte bei Terminal Servern löst. Mit der ebenfalls angebotenen Streaming Technologie (siehe 3.3) wird ein neues Kapitel bei der automatischen Softwareverteilung aufgeschlagen, das Anbietern im Terminal Server Bereich wie z.B. Citrix zu Nutze kommen oder aber auch zum Verhängnis werden kann. Microsoft erkannte das Potential der *Softgrid* Plattform und gab am 22. Mai diesen Jahres die geplante Übernahme von Softricity bekannt (vgl. Mic06a). Auf die Gründe Microsofts für die Übernahme bzw. die Möglichkeiten, die Microsoft bei der Integration von Applikationsvirtualisierung und Streaming in seine Produkte hat, wird in den nächsten Kapiteln eingegangen.

Gerade durch die Herausforderung an Citrix ständig neue Verkaufsanreize zu schaffen, verließ die Firma in den letzten Jahren immer mehr ihr Kerngeschäft und kaufte Firmen aus anderen Bereichen auf. Ein sehr erfolgreicher Schritt war dabei Ende 2004 der Kauf des SSL-VPN Anbieters Net6, dessen Lösung sehr ausgereift war und Citrix damit erfolgreich am Markt für SSL-VPNs etablierte. Der Schritt war Teil einer Strategie Richtung "Access", also dem sicheren und intelligenten Zugang zu Applikationen, der in Kapitel 3.4 beschrieben wird.

3.1 Virtualisierung

Virtualisierung ist eines der wichtigsten Schlagworte der letzten Jahre. Je nach Hersteller und Kontext bedeutet der Begriff etwas ganz Unterschiedliches. Allgemein bezeichnet es ein Verfahren, mit dem die Ressourcen eines Computers aufgeteilt werden können.

Die technische Funktionsweise von Virtualisierung ist natürlich davon abhängig, welche Ressource auf welche Weise virtualisiert werden soll. Es gibt ganz unterschiedliche Begriffe wie Speichervirtualisierung, Prozessorvirtualisierung, Hardwarevirtualisierung oder Softwarevirtualisierung.

In diesem Kapitel soll nur die für Terminal Services bedeutende Virtualisierung des Betriebssystems auf Servern und die Virtualisierung von Applikationen auf einem Rechner besprochen werden. Die Verfahren unterscheiden sich in ihrer Funktionsweise, auch wenn die zu Grunde liegende Idee die Gleiche ist.

Die Ressourcen werden vom darunter liegenden System abgekoppelt und laufen in einer logischen Zwischenebene. Für die Ressourcen ist dies nicht erkennbar. Die Vorteile einer solchen Lösung werden in den folgenden Kapiteln aufgezeigt.

3.1.1 Servervirtualisierung

Die Auslastung von Servern in einem Rechenzentrum ist in der Regel nicht optimal. Einige Dienste wie z.B. Datenbankserver, Lizenzserver oder Mailserver nutzen nur einen Bruchteil der eigentlichen Hardwareressourcen des Servers. Trotzdem ist es nicht empfehlenswert mehrere Dienste auf dem gleichen physikalischen Rechner zu installieren, da die Dienste sich gegenseitig in die Quere kommen könnten (vgl. Bod05, S.423).

Hat ein Dienst einen Fehler und bringt das Betriebssystem zum Absturz, sind auch die anderen Dienste, die auf dem gleichen Rechner installiert sind, nicht mehr erreichbar. Ein weiteres Problem ist die benötigte Redundanz bei Diensten. Es werden in vielen Fällen Backup Server betrieben, die bei einem Fehler des eigentlichen Servers den Dienst weiterhin anbieten können, damit es nur zu kurzen oder gar keinen Ausfallzeiten kommt.

Allerdings ist die Anschaffung und Wartung der Server bzw. die Hardware mit hohen Kosten verbunden. Eines der wichtigsten Einsatzgebiete von Virtualisierung ist deswegen die Virtualisierung des Betriebssystems auf Servern. Damit können mehrere virtuelle Maschinen mit unterschiedlichen Betriebssystemen auf einer physikalischen Maschine betrieben werden (vgl. Bod05, S.435).

Es gibt dabei zwei Ansätze, die anhand der Produkte *VMWare Server* bzw. *Virtual Server 2005* von Microsoft und *ESX Server* von VMWare im Folgenden erklärt werden. Beim *Virtual Server* bzw. *VMWare Server* setzen die virtuellen Maschinen auf einem vorhandenen Betriebssystem auf. Die Virtualisierungs-Software wird also z.B. auf einer existierenden Version von Windows Server 2003 installiert und kann dann mehrere virtuelle Maschinen erstellen, auf denen wiederum ein ausgewähltes Betriebssystem wie Linux oder Windows installiert werden kann (siehe Abbildung 3.1). Die virtuellen Maschinen sind zwar voneinander getrennt, doch sollte das zu Grunde liegende Betriebssystem ausfallen, stoppen auch alle virtuellen Maschinen (vgl. Bod05, S.428).

Der bei VMWares *ESX Server* verfolgte Ansatz ist der für den Betrieb solidere und professionellere. *ESX* enthält das zu Grunde liegende Betriebssystem selbst und wird direkt auf dem Server installiert. Die mit *ESX* betriebenen virtuellen Maschinen können damit unabhängig voneinander gestartet und gestoppt werden und sind damit komplett getrennt voneinander (siehe Abbildung 3.2). Außerdem ist der Geschwindigkeitsverlust gegenüber einem normal installierten Betriebssystem minimal. Ganz anders bei einer Lösung mit *Virtual Server* oder *VMWare Server*, wo beim Einsatz mit Terminal Servern 30 bis 40 Prozent Overhead entstehen. Für Terminal Server Farmen eignet sich damit nur der *ESX Server* (vgl. OM06).

Die bessere Ausnutzung der physikalischen Ressourcen ist aber nicht das einzige Argument für Virtualisierung. Mit der *VMotion* Technologie für *ESX* von VMWare können virtuelle Maschinen im laufenden Betrieb einfach zu einem anderen physika-

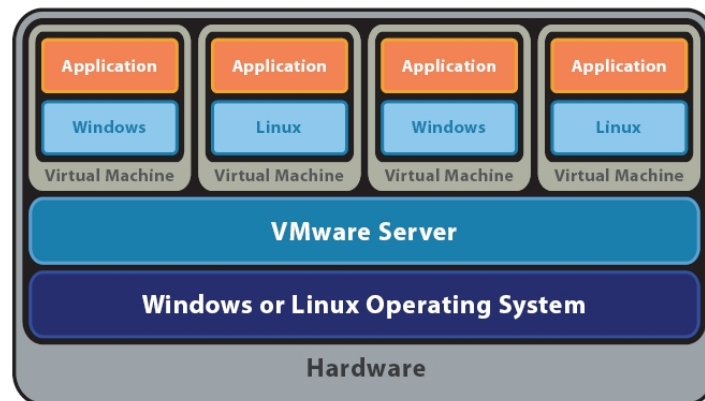


Abb. 3.1: *VMWare Server* benötigt wie der *Microsoft Virtual Server* ein Wirt-Betriebssystem auf dem die virtuellen Maschinen laufen.
Quelle: VMWare

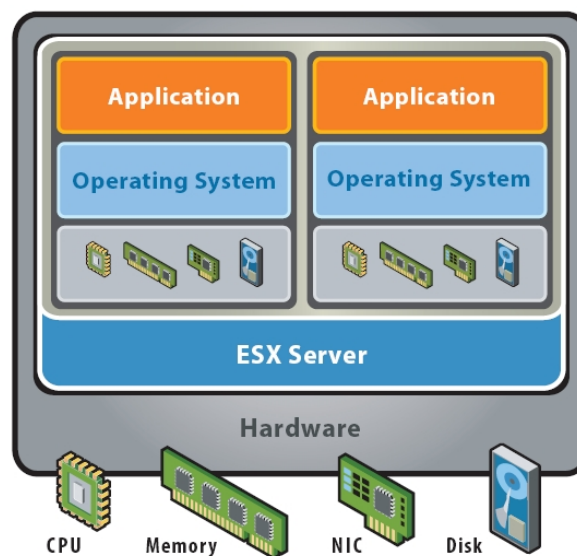


Abb. 3.2: Beim *ESX Server* laufen die virtuellen Maschinen ohne Wirt-Betriebssystem direkt auf dem Rechner. Quelle: VMWare

lischen Server verschoben werden. Das bedeutet, wenn ein physikalischer Server ausfällt oder gewartet werden muss, können Dienste komplett mit dem darunter liegenden Betriebssystem im laufenden Betrieb vorrübergehend auf einen anderen Server geschoben werden (vgl. [VMw06c](#)). Dadurch kann eine Ausfallzeit des Dienstes vermieden werden.

Die Möglichkeiten der Virtualisierung von Servern bietet den Betreibern von Terminal Servern viele Vorteile. Terminal Server haben eine Schwäche bei der Ausnutzung der Server Ressourcen. Die maximale Anzahl der parallelen Benutzer erhöht sich nicht linear mit der Anzahl der Prozessoren oder der Größe des Hauptspeichers. Ein normal ausgestatteter Server mit zwei Prozessoren unterstützt durchschnittlich ca. 100 Benutzer. Wird auf vier Prozessoren verdoppelt, können ca. 200 Benutzer gleichzeitig auf dem Terminal Server arbeiten. Bei sechs Prozessoren stagniert die Anzahl allerdings bei 210 Benutzern und selbst der modernste Server mit acht Prozessoren kann nur 220 Benutzer unterstützen (vgl. [Mad03a](#)).

Der Grund dafür ist die Abhängigkeit der Terminal Server vom Betriebssystemspeicher, der bei Windows Server 2003 auf 2 GB begrenzt ist. Der Betriebssystemspeicher läuft beim gleichzeitigen Betrieb von mehreren Benutzersessions voll, unabhängig von der Rechenleistung oder der Größe des Hauptspeichers.

Durch die Nutzung von mehreren virtuellen Maschinen mit jeweils einer Installation von Windows Server 2003 auf einem sehr leistungsstarken Server, kann die Zahl der Benutzer um ein vielfaches erhöht werden. Je nach Art der Applikationen, die betrieben werden, kann ein mit vier Prozessoren ausgestatteter Rechner, auf dem vier virtuelle Maschinen betrieben werden, bis zu 400 Benutzer unterstützen.

Zusätzlich kommt einer auf virtuellen Maschinen betriebenen Terminal Server Umgebung ebenfalls die oben beschriebene *VMotion* Funktionalität und die Ausfallsicherheit durch das einfache Betreiben von Backup Servern zu Gute. Insgesamt wird die Auslastung der Hardware verbessert und existierende Server können effizienter eingesetzt werden.

Virtualisierung bietet aber auch in gewissen Fällen eine Alternative zu Terminal Services. Angenommen es wird kein Server Betriebssystem, sondern eine Workstation Version von Windows XP installiert. Die Benutzer können sich damit beispielsweise von einem Thin Client auf ihren eigenen virtuellen Rechner im Datenzentrum mit der bei Windows enthaltenen Remote Desktop Funktionalität bzw. RDP (vgl.

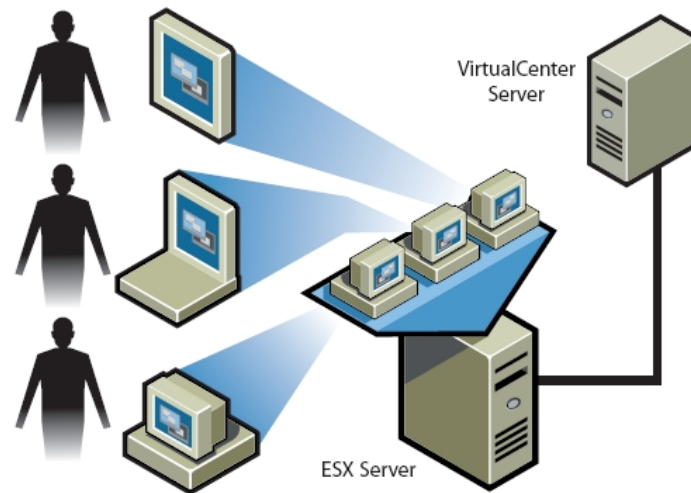


Abb. 3.3: Bei virtuellen Desktops können mehrere Benutzer auf einem Server in ihrer eigenen virtuellen Umgebung arbeiten.
Quelle: VMWare

Kapitel 2.4.2) verbinden. Genau diese Lösung fördert VMWare mit ihrer Virtual Desktop Infrastructure (=VDI) (vgl. VMW06b), bei der die virtuellen Maschinen zentral verwaltet werden können und somit die Zeit für die Wartung der Desktops von Benutzern reduziert werden kann (siehe Abbildung 3.3).

Gleichzeitig gelten bei der Mobilität die selben Vorteile wie bei Terminal Services. Benutzer können von überall, auch von unterwegs, auf ihren Desktop zugreifen. Die Sicherheit beim Zugriff ist gegeben, da der Administrator gegebenenfalls genau festlegen kann, was auf der virtuellen Maschine installiert ist.

VDI ist gerade dann sinnvoll, wenn Anwendungen genutzt werden sollen, die nicht mehrbenutzerfähig sind bzw. die nicht auf einem Terminal Server lauffähig sind. Für z.B. Entwickler, die lokale Adminrechte benötigen um neue Software zu installieren oder ihren Rechner neu starten müssen, bietet VDI die nötigen Freiheiten im Gegensatz zu Terminal Services. Der virtuelle Desktop kann, wie ein normaler PC, nach Belieben angepasst werden ohne möglicherweise andere Benutzer zu beeinflussen (vgl. Zie06).

Bei VDI muss im Gegensatz zu Terminal Services für jeden zur Verfügung gestellten Desktop ein eigenes Betriebssystem installiert sein (siehe Abbildung 3.4). Die Installation und das Updaten von Applikationen ist trotz Hilfsmittel umständlicher

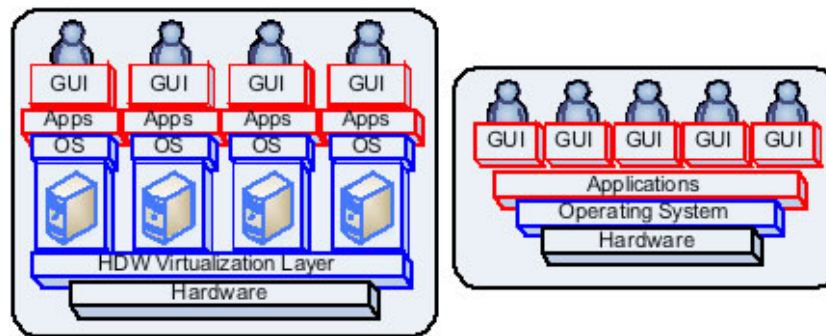


Abb. 3.4: Vergleich der Architektur von VDI (links) mit der eines Terminal Servers (rechts).

Quelle: Brian Madden

als bei Terminal Services, wo die Anwendung nur ein einziges Mal installiert werden muss, um für verschiedene Benutzer freigegeben werden zu können. Außerdem können nur komplette Desktops verwendet werden und keine publizierten Anwendungen wie in einer Citrix Umgebung. Bei intensivem Datenaustausch zwischen virtuellem Desktop und Client, wie z.B. bei einem Datentransfer, leidet die Bandbreite des Netzwerkes. Wie bei Terminal Services ist kein Offlinebetrieb möglich. Die Benutzer müssen eine Netzwerkverbindung haben (vgl. [Zie06](#)).

Gerade im Zusammenhang mit kostengünstigen Blades (vgl. Kapitel [3.2.1](#)) und der Möglichkeit den Desktop eines Benutzers z.B. je nach Auslastung eines Servers von diesem Server auf einen anderen Server zu verschieben, bietet Virtualisierung eine große Flexibilität und Skalierbarkeit bei der Bereitstellung von Desktops für die Benutzer.

Virtualisierung gibt es nicht nur auf der Seite der Server, sondern auch bei PCs. Auf einem PC können damit in virtuellen Umgebungen mehrere Betriebssysteme laufen, was z.B. für den Test von Applikationen unter verschiedenen Rahmenbedingungen benutzt werden kann. Ein im Kapitel [3.4](#) genauer beschriebenes Anwendungsgebiet ist die Assured Computing Environment, bei der von einer auf dem PC laufenden virtuellen Umgebung auf das Firmennetzwerk zugegriffen wird.

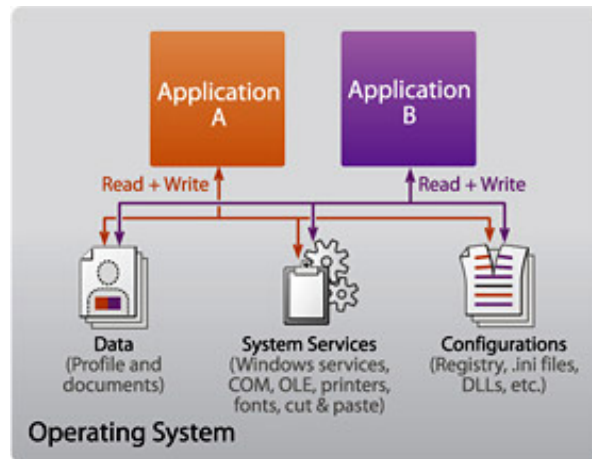


Abb. 3.5: Bei einer traditionellen Installation hat die Anwendung Zugriff auf Komponenten des Betriebssystems. Quelle: Softricity

3.1.2 Applikationsvirtualisierung

Wie in Kapitel 2.5.1 beschrieben, ist eines der großen Mankos bei Terminal Services das mögliche Auftreten von Konflikten zwischen mehreren installierten Applikationen. Applikationsvirtualisierung, wie sie z.B. von Softricity mit *Softgrid* angeboten wird, löst diese Problematik. Dank dieser Technologie hat die Installation einer Anwendung keine Auswirkung auf den Zustand des Betriebssystems. Jede Applikation läuft in ihrer eigenen Umgebung und kann von globalen Komponenten lesen, sie aber nicht verändern (siehe Abbildungen 3.5 und 3.6).

So ist ein reibungsloser Betrieb vieler Applikationen möglich, was gerade bei Terminal Servern, auf denen in der Regel eine Vielzahl an Anwendungen installiert ist, von großem Vorteil ist. Softgrid bildet eine abstrahierte Ebene zwischen Betriebssystem und Applikation. Alle kritischen Komponenten wie die Registrierungsdatenbank, Konfigurationsdateien wie INI oder DLL, Windowsdienste, Dateien, Profile oder das Dateisystem werden virtualisiert, d.h. jede Applikation schreibt z.B. in ihre eigene Registrierungsdatenbank.

Betriebssystem und Applikation sind damit komplett getrennt. Falls Informationen aus einer globalen Betriebssystem Komponente benötigt werden, liest die Zwischenschicht diese aus dem Betriebssystem und stellt sie in der virtualisierten Umgebung der Applikation zur Verfügung.

Damit kann eine neue Anwendung auf den Terminal Server gebracht werden, ohne vorher das Zusammenspiel mit bereits installierten Anwendungen zu testen.

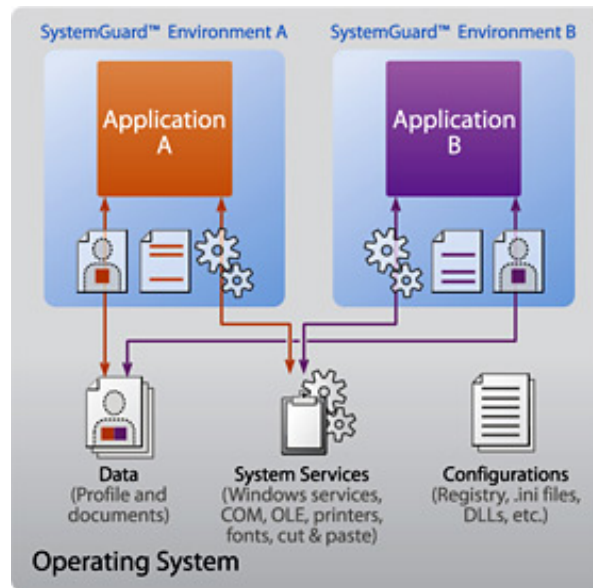


Abb. 3.6: In einer virtuellen Umgebung hat die Applikation keinen schreibenden Zugriff auf das Betriebssystem. Quelle: Softricity

Zusätzlich wird die Performanz des Systems gesteigert. Normalerweise wird das System umso langsamer, je mehr Anwendungen installiert sind. Da aber die Einträge in der virtuellen Umgebung auf die installierte Applikation begrenzt bleibt und das Betriebssystem nicht verändert wird, ist die Geschwindigkeit auch bei einer Vielzahl von Anwendungen nahezu noch unverändert.

Da Microsoft Pläne zur Übernahme von Softricity (vgl. [Mic06a](#)) bekannt gegeben hat, kann spekuliert werden, ob Applikationsvirtualisierung in naher Zukunft in einer ähnlichen Form im Windows Betriebssystem enthalten sein wird.

Um Applikationskonflikte zu vermeiden, hat auch Citrix eine Lösung für den reibungslosen Betrieb mehrerer Applikationen. Bei der Application Isolation Environment (=AIE) handelt es sich aber genau genommen um keine wirkliche Virtualisierung. AIE beinhaltet die Umleitung von wichtigen Komponenten in geschützte Bereiche. Dafür werden Applikationen mit Hilfe der AIE installiert und gestartet. Benötigte Registrierungseinträge und Konfigurationsdateien werden bei der Installation aufgezeichnet und schließlich im Betrieb in den richtigen Bereich weitergeleitet.

Der große Unterschied ist, dass die Applikationen immer noch direkten Zugriff auf das Betriebssystem haben (wenn auch in ihrem eigenen Bereich). Außerdem grei-

fen die Applikationen immer noch auf die gleichen Windows Betriebssystem Dienste, wie Druckertreiber usw. zu. Bei *Softgrid* werden im Gegensatz dazu die Anwendungen in einer Zwischenschicht betrieben.

Ein weiterer Unterschied ist, dass AIE hauptsächlich für Server bzw. Terminal Server ausgelegt ist, während *Softgrid* sowohl auf dem Server als auch auf einem Desktop PC betrieben werden kann.

AIE ist beim *Presentation Server* enthalten und somit eine kostengünstige Lösung um Konflikte zwischen Anwendungen zu vermeiden. Die Citrix Lösung hat aber, wie oben beschrieben, klare Grenzen und viele Nachteile gegenüber einer wirklichen Applikationsvirtualisierung mit *Softgrid*.

3.2 Blade Technologie

Während Virtualisierung die geteilte Benutzung von Hardware ermöglicht, gehen Blades bei der Skalierung in die andere Richtung. Sie ermöglichen das flexible Hinzufügen, Entfernen und Verschieben von Rechenleistung in einer Serverfarm.

Zusätzlich sparen Blades Platz und Strom. Kein Wunder also, dass alle großen Serverhersteller wie IBM, HP, Dell usw. inzwischen Bladelösungen anbieten. Weitere Argumente für einen Kauf sind wie z.B. bei Egenera eine zentrale Verwaltung aller Ressourcen und die Virtualisierung auf Hardwareebene. Dies führt zur noch flexibleren Aufteilung der Rechenleistung zwischen laufenden Diensten.

Die nächsten Kapitel stellen die Blade Technologie vor und zeigen ihre Bedeutung im Einsatz mit Terminal Servern. Bei Bladed PCs handelt es sich um ein konkurrierendes Konzept, welches Vor- und Nachteile gegenüber Terminal Services hat.

3.2.1 Blade Server

Ein Blade ist ein kompaktes Einschubmodul mit Prozessoren und Hauptspeicher (siehe Abbildung 3.7). Blades werden in ein Chassis eingebaut, das mit einer Backplane versehen ist, die Netzwerkfunktionen und Strom liefert. Damit teilen sich die Blades eine Stromzufuhr und die gleiche Kühlung. Im Bestfall gibt es keine sichtbare Verkabelung der Blades im Chassis. Sämtliche Netze, ob Ethernet, Fibre Channel, Infiniband oder sonstiges nebst Hubs, Switches und Bridges sollen über im Inneren verborgene Verbindungen laufen (vgl. Hül06).



Abb. 3.7: Beispiel für ein Blade:
HP ProLiant BL25p Server Blade. Quelle: HP

Eine Blade Plattform rentiert sich laut den Marktforschern von IDC erst, wenn ein Chassis mindestens zur Hälfte gefüllt ist. Diese Rechnung gilt demnach, wenn ein halbvolles Chassis ungefähr 6 bis 8 herkömmliche Server ersetzt. Beim heute angenommenen, durchschnittlichen Gebrauch rechnen die Analysten bei einem Server mit 10 bis 15 Nutzern. Also könnte ein mittelständisches Unternehmen mit 500 Arbeitsplätzen 30 bis 40 traditionelle Server durch zwei bis drei Blade Plattformen ersetzen (vgl. [Sch06b](#)).

Neben der Platzersparnis und den Einsparungen an Strom, ist besonders die Skalierbarkeit einer Blade Plattform hervorzuheben. "Zu den hauptsächlichen Verlockungen der Blade-Technik zählt die versprochene einfache Auswechselbarkeit. Das Wort vom Hausmeisterservice ging um: Jeder soll mal eben auf einen Anruf hin einen defekten Server austauschen können - die defekte Blade ausschalten, herausziehen und eine neue aus dem Schrank holen, einstecken und wieder einschalten. Alles weitere geschieht danach automatisch - so die Idee" (vgl. [Hül06](#)). Durch verschiedene Management-Tools, die je nach Anbieter unterschiedlich sind, ist es möglich mehrere Blades als Einheit anzusprechen, jedes Blade per Remote Control zu administrieren und Parameter wie Temperatur oder CPU Spannung zu überwachen (vgl. [Gru06](#)). Damit werden die Kosten für die Wartung gesenkt.

Sehr interessant ist die Lösung von Egenera, bei der es möglich ist Prozessoren und Hauptspeicher im laufenden Betrieb hinzuzufügen oder zu entfernen. Darüber

hinaus können mehrere Blades zu einem logischen Server zusammengeschlossen werden. Es findet also eine Virtualisierung auf der Hardwareebene statt, die es ermöglicht, einem logischen Server bzw. dem Dienst, der darauf läuft, dynamisch Rechenleistung zuzuordnen oder davon zu entfernen (vgl. [Hül05](#)).

Wird der Gedanke weitergeführt, dann bekommt jeder Dienst dynamisch genauso viel Rechenleistung zugeordnet, wie er im Moment benötigt. Ist der Dienst nicht in Benutzung, kann er seine Rechenleistung einem anderen Dienst "ausleihen". Wichtig ist dabei natürlich auch ein effizientes Management der Ressourcen durch Administrationssoftware (vgl. [Mad05b](#)).

Für Terminal Server bieten Blades ein hohes Maß an Skalierbarkeit der Leistungsfähigkeit. In einer Terminal Server Farm kann je nach Auslastung Kapazität neu hinzugefügt oder neu verteilt werden.

3.2.2 Bladed PC

Im letzten Kapitel wurde noch nicht ersichtlich, warum Blades für den Terminal Server Markt besonders wichtig sind. Allein der Grund, dass eine Terminal Server Farm auf Blades laufen kann und damit die Skalierbarkeit des Systems erhöht wird, ist noch keine wirkliche Innovation.

Was allerdings als wirkliche Alternative zu Terminal Services angesehen werden kann, ist das Konzept der Bladed PCs, das von Firmen wie HP mit der Consolidated Client Infrastructure (vgl. [HP06](#)) und ClearCube (vgl. [Cle06](#)) angeboten wird.

Bei den Bladed PCs (siehe Abbildung [3.8](#)) erhalten die Benutzer ihr eigenes Blade in einem Chassis (siehe Abbildung [3.9](#)) im Datenzentrum, auf das sie mit einem Thin Client (siehe Kapitel [2.6.1](#)) zugreifen. Der Desktop PC der Mitarbeiter wandert also in das Datenzentrum.

Vorteile sind neben der einfachen zentralen Wartung (siehe Abbildung [3.10](#)) der Bladed PCs, die schnelle Reaktionszeit bei Fehlern, denn ein Blade lässt sich leicht austauschen im Gegensatz zu einem Desktop PC. Die Benutzer können von überall auf ihr Blade zugreifen, auch von unterwegs. Die Benutzer haben eine größere Freiheit als bei Terminal Services, da sie auf ihrem Blade beliebige Einstellungen vornehmen und unterschiedliche Anwendungen installieren können, ohne dass es zu Konflikten mit anderen Benutzern kommen kann. Da die Rechenleistung pro Be-

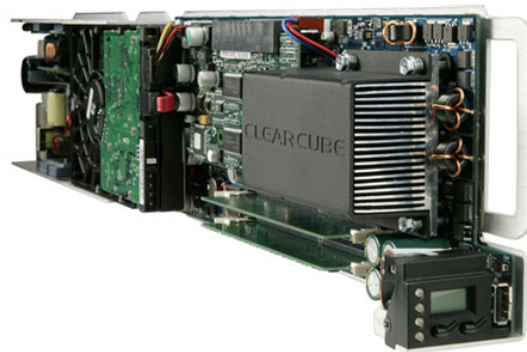


Abb. 3.8: Ein PC Blade von ClearCube. Quelle: ClearCube



Abb. 3.9: Das Chassis im Datenzentrum für die PC Blades.
Quelle: ClearCube

nutzer konstant ist, eignen sich Bladed PCs besonders für sehr rechenintensive Programme, die einen Terminal Server unter Umständen in die Knie zwingen würde.

Doch hat auch diese Lösung Nachteile. Für jeden Mitarbeiter sind eigentlich zwei Rechner erforderlich, der Bladed PC und der Thin Client. Thin Clients können zwar nahezu unbegrenzt lange ohne Austausch verwendet werden, doch sind die insgesamt anfallenden Anschaffungskosten abschreckend hoch. Die Benutzer benötigen immer eine Netzwerkverbindung um ihr Blade nutzen zu können. Applikationen werden auf jedem Blade einzeln installiert und auf jedem Blade können unterschiedliche Probleme auftreten. Damit ist der Aufwand für die Wartung um einiges höher (vgl. [Mad04c](#)).

Eine Mischung aus den verschiedenen Technologien ist in einigen Fällen die beste Lösung. Angenommen es gibt in einer Firma ein sehr rechenintensives Grafikprogramm, das den vorhandenen Terminal Server fast komplett auslastet. Hier wäre es besser dieses Programm stattdessen über einen Bladed PC bereit zu stellen und den Benutzern den Zugang zu dem Blade als publizierte Anwendung in Citrix zur Verfügung zu stellen.

Die Möglichkeiten, die sich durch den Einsatz von Virtualisierung im Zusammenhang mit Bladed PCs ergeben, sind ebenfalls interessant. Wie in Kapitel [3.1.1](#) beschrieben, könnten auf einem Server mehrere virtuelle Desktops für Benutzer bereit gestellt werden.

Statt jedem Benutzer seinen eigenen Bladed PC zur Verfügung zu stellen, könnte auch mehrere virtuelle Maschinen auf dem Blade erstellt werden. So teilen sich mehrere Mitarbeiter ein Blade und die Hardwarekosten können gesenkt werden. Selbst bei vielen Mitarbeitern nehmen die Blades dank der Kompaktheit in den Chassis wenig Platz ein und für den Administrator sind sie leichter zu verwalten als traditionelle Server (vgl. [BS06](#)).

3.3 Streaming Technologie

Viele Firmen bevorzugen den Einsatz einer automatischen Softwaredistribution (siehe Kapitel [2.5.3](#)) an Stelle von Terminal Services. Durch die automatische Verteilung von Software kann sichergestellt werden, dass der Benutzer eine fehlerfreie Anwendung in der richtigen Version erhält, ohne dass der Administrator oder der Benutzer diese

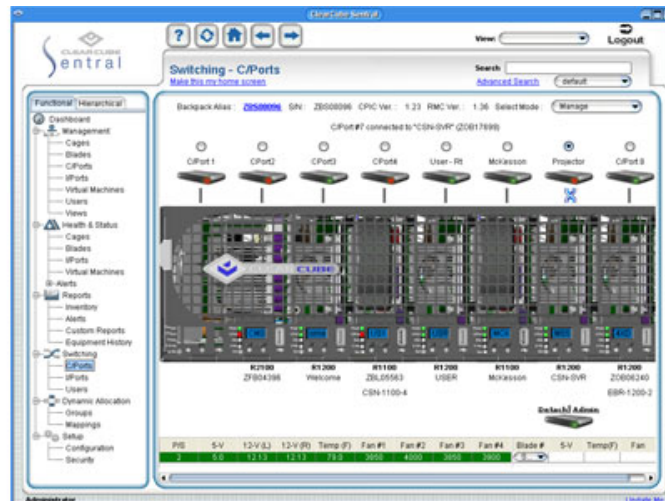


Abb. 3.10: Mit der Managementsoftware lässt sich der Zustand der Blades überwachen und Einstellungen vornehmen.
Quelle: ClearCube

auf jedem PC per Hand installieren muss. Außerdem sind die meisten Firmen bereits mit traditionellen Desktop PCs für ihre Mitarbeiter ausgestattet und sehen deswegen keinen Nutzen im Einsatz von Terminal Services bzw. einer Umstellung auf Thin Clients.

Das Streaming von Applikationen ist im Ansatz ähnlich zur gewohnten automatischen Verteilung mit z.B. Microsofts SMS, bietet aber sehr wichtige Verbesserungen. Softricitys *Softgrid* Plattform verbindet Applikationsvirtualisierung (siehe Kapitel 3.1.2) mit Applikationsstreaming und hat damit ein mächtiges Konkurrenzprodukt im Portfolio. Diese Verbesserungen waren wohl auch Microsoft wichtig, denn, durch die schon oben erwähnte geplante Übernahme von Softricity durch Microsoft, wird die *Softgrid* Technologie wohl bald auch im Systems Management Server zu finden sein (vgl. MWM06).

Beim Streaming wird die Applikation durch einen Sequencer in ein virtuelles Anwendungspaket umgewandelt (siehe Abbildung 3.11). Dabei werden alle notwendigen Informationen (Registrierungseinträge, DLLs, Dateien, Variablen) einer Applikation in eine Datei gepackt. Diese Datei wird auf einen oder mehrere *Softgrid* Server gelegt und für bestimmte Benutzergruppen freigegeben (vgl. Sof06b).

Startet ein Benutzer die für ihn freigegebene Applikation, wird die Anwendungs-

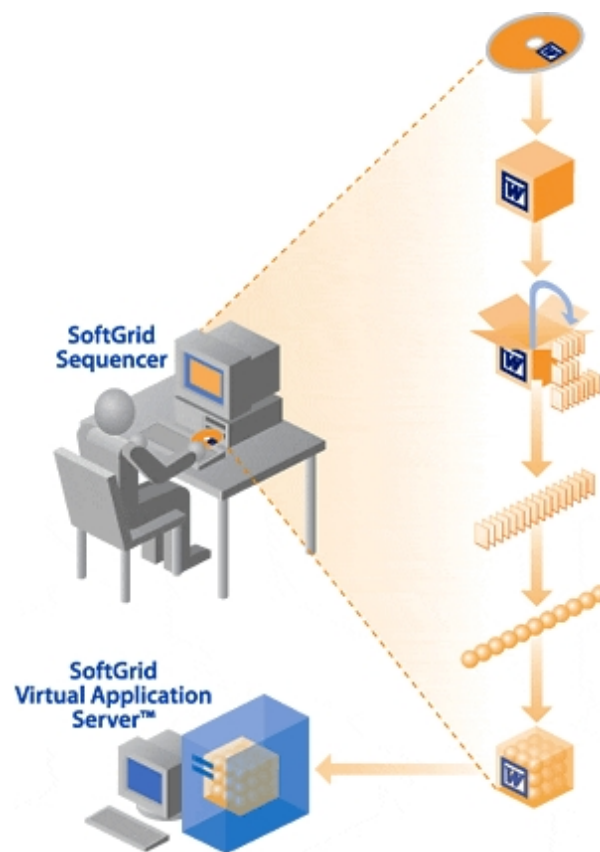


Abb. 3.11: Mit dem Sequencer kann ein Anwendungspaket erstellt werden, das paketweise zum Client geschickt werden kann. Quelle: Softricity

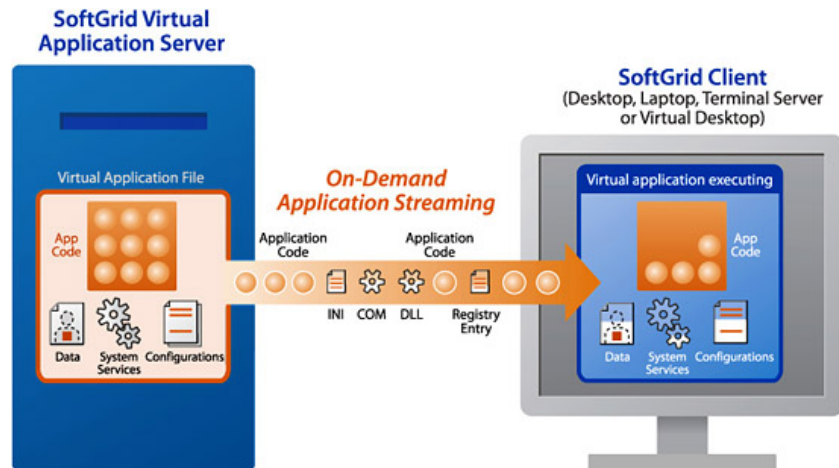


Abb. 3.12: Das erstellte Applikationspaket läuft beim Client in einer virtuellen Umgebung. Quelle: Softricity

datei paketweise zum Client übertragen. Dabei werden zuerst nur die Pakete übertragen, die zum Start notwendig sind (je nach Anwendung 20 bis 40 Prozent). Bei Bedarf werden die restlichen Pakete im laufenden Betrieb nachgeladen (vgl. [Sof06c](#)).

Das Applikationspaket läuft am Client in der in Kapitel 3.1.2 beschriebenen virtuellen Umgebung (siehe Abbildung 3.12). Dafür ist eine *Softgrid* Software auf dem Client erforderlich. Somit kann es zu keinen Konflikten zwischen den Applikationen kommen und es werden keine Einstellungen des Betriebssystems auf dem Client durch die Anwendungen verändert. Die Einstellungen des Benutzers für die Anwendung werden auf dem *Softgrid* Server gespeichert, sodass der Benutzer beim Start der Anwendung von einem anderen Clientgerät seine Einstellungen wieder vorfindet (vgl. [GM06](#)).

Diese Technologie vereint damit Stärken der automatischen Softwaredistribution mit denen des Server Based Computing. Anwender können von jedem Rechner aus auf ihre Anwendungen zugreifen. Im Gegensatz zu Terminal Services ist auch ein Offlinebetrieb der Programme möglich, da die Pakete auf den Rechner transferiert werden. Der Administrator muss eine Applikation nur einmal sequenzieren und auf den *Softgrid* Server stellen, um sie für alle Benutzer verfügbar zu machen.

Der Vorteil, der sich durch die virtualisierte Umgebung ergibt, kann für Updates und zur Fehlerbehebung genutzt werden. Updates für Anwendungen sind sehr einfach zu verteilen. Es wird ein aktualisiertes Applikationspaket erstellt und veröf-

fentlicht. Beim nächsten Start der Applikation durch den Benutzer, werden die vorhandenen Pakete gelöscht und die neuen Pakete der Anwendung vom Server geladen. Falls eine Applikation einen Fehler hat, kann ein "Reflush", also die Löschung aller Dateien und Einstellungen der Anwendung, durchgeführt und ein neues, funktionsfähiges Paket geholt werden.

Mit der Zusatzfunktionalität von *ZeroTouch* bietet Softricity zum einen ein Webinterface, mit dem ein Benutzer alle für ihn freigegebenen Anwendungen über einen Webbrowser ansteuern kann. Zum anderen können sich mit *ZeroTouch* Benutzer aus einem Pool von Applikationen benötigte Programme aussuchen und, nachdem ein Genehmigungsworkflow durchlaufen ist, starten. Softricity nennt dieses System "End-user self-service provisioning" (vgl. [Sof06d](#)).

Die Datenmengen, die über das Netzwerk übertragen werden, sind viel größer als bei einem Präsentationsprotokoll wie RDP oder ICA, da ja nicht nur Bildschirmhalte, sondern komplette Programmteile versendet werden. Über das Internet mit einer Verbindung mit wenig Bandbreite ist dieses System natürlich ungeeignet. Deshalb sieht *ZeroTouch* auch den komplementären Einsatz von Terminal Services vor. Anhand von Parametern wie Bandbreite, IP Adresse, Clientname usw. wird entschieden, ob die Applikation an den Client per Stream übertragen werden soll, oder ob der Benutzer auf einen *Presentation Server* umgeleitet werden soll und dort die Applikation startet (vgl. [GM06](#)).

Der *Presentation Server* muss dafür die Anwendung nicht einmal installiert haben, sondern bekommt einfach das Applikationspaket vom *Softgrid* Server bei Bedarf zugesendet. Voraussetzung ist natürlich, dass der *Presentation Server* einen *Softgrid* Client besitzt. Es können beliebig viele Applikationen vom *Presentation Server* zur Verfügung gestellt werden, ohne dass die Leistung des Systems reduziert wird bzw. Konflikte zwischen den Applikationen entstehen. Für Updates und Fehlerbehebung muss keine neue Installation auf dem *Presentation Server* erfolgen, sondern, wie oben beschrieben, einfach eine neue Version aus dem *Softgrid* Applikationspool geholt werden.

Da *Softgrid*, ähnlich wie der Citrix *Presentation Server*, eine nahtlose Integration der sich auf dem Server befindenden Anwendungen unterstützt, werden, wie gewohnt, Startmenüeinträge oder Desktop Icons beim Benutzer angezeigt. Damit mischen sich Online- und Offlinenutzung von Anwendungen, ohne dass der Benutzer etwas davon merkt. Je nachdem aus welcher Umgebung der Benutzer die Verbindung zum

Server aufnimmt, wird die Applikation gestreamt und auf dem Client ausgeführt oder auf dem Server gestartet und die Bildschirminhalte werden übertragen (vgl. [GM06](#)).

Auch für den SMS ergeben sich viele Vorteile. Softricity bietet die *Softgrid* Plattform auch speziell in einer Microsoft SMS Edition an. In dieser Edition wird die komplette Konfiguration weiterhin über die SMS Management Console durchgeführt. Es können entweder Applikationspakete zu den Clients gestreamed oder MSI Installationspakete übertragen und installiert werden. In beiden Fällen laufen die Applikationen in einer virtualisierten Umgebung auf dem Client. Der Umstieg kann also langfristig erfolgen, da nicht alle MSI Pakete sofort mit *Softgrid* Paketen ausgetauscht werden müssen. Wie im oben beschriebenen Zusammenspiel zwischen *Presentation Server* und *Softgrid* Server, bekommt auch der SMS angeforderte Applikationspakete nach Bedarf vom *Softgrid* Server und leitet diese je nach Einstellung der Berechtigungen an bestimmte Benutzergruppen (vgl. [Sof06a](#)).

Diese Funktionalität von Softricity als Zusatzanbieter wird Microsoft nach der Übernahme vorraussichtlich in das SMS Basisprodukt integrieren. Durch die Übernahme wird die im kleinen Kreis hoch gelobte Applikationsvirtualisierung und das Applikationsstreaming eine lohnende Technologie für die breite Masse (vgl. [MWM06](#)).

Abschließend sollte noch erwähnt werden, dass auch Citrix eine Streaming Technologie in der Entwicklung hat. Mit dem Projekt *Tarpon*, das schon im Oktober 2005 erstmals vorgestellt wurde, drängt Citrix ebenfalls in den Markt zur automatischen Softwaredistribution (vgl. [Mad04a](#)). Ähnlich wie bei der Softricity Lösung, sollen Applikationen je nach Verbindung gestreamed oder auf dem *Presentation Server* ausgeführt werden. Allerdings ist immer noch kein konkretes Produkt mit dieser Technologie angekündigt und durch die Übernahme von Softricity durch Microsoft dürfte Citrix erheblichen Gegenwind spüren (vgl. [MWM06](#)).

3.4 Secure und Smart Access

Um sich am Markt behaupten zu können weitet Citrix seinen Geschäftsbereich immer weiter aus. Um nicht zu sehr vom Produkt *Presentation Server* bzw. den dazugehörigen Lizenzen, die den Löwenanteil ihres Umsatzes ausmachen, abhängig zu sein, kaufte Citrix in der letzten Zeit eine Vielzahl an Firmen auf.

Eine dieser Firmen war Net6, ein SSL-VPN Anbieter, dessen Lösung sehr ausgereift ist und dessen Technologie bei Citrix unter dem Namen *Access Gateway* als Produkt angeboten wird. Das *Access Gateway* ist Teil der neuen Strategiewendungsrichtung im Zeichen von "Access", also dem sicheren und intelligenten Zugang zu Applikationen. Damit wird Citrix nicht nur Anbieter von Lösungen zur Bereitstellung der Applikationen, sondern auch von Komponenten für die benötigte Infrastruktur. Das *Access Gateway* kann im Grunde genommen auch ohne *Presentation Server* eingesetzt werden (vgl. Cit04).

Damit steht Citrix nun neuerdings in Wettbewerb mit Netzwerkausrüstern wie Juniper oder Cisco. Der eigentliche Vorteil bei der von Citrix angebotenen Lösung ist vor allem die nahtlose Integration des *Presentation Servers* mit dem *Access Gateway* und dem Produkt *Advanced Access Control* (=AAC), das später besprochen wird. Damit kann eine viel feinere Zugangskontrolle zu Applikationen, Daten und Netzwerkressourcen umgesetzt werden, als bei klassischen VPNs.

Das *Access Gateway* beinhaltet sowohl eine Software als auch eine Hardware Komponente. Die Hardware ist ein typischer Server, auf dem eine abgespeckte Version von Linux läuft. Die eigentliche *Access Gateway* Software wird auf dieser mitgelieferten Server Box installiert. Citrix vertreibt das *Access Gateway* nur in dieser Form, auch wenn es theoretisch möglich wäre, die Software auf jeden beliebigen Rechner zu installieren (vgl. Mad06c).

Die zwei Aufgaben, die dem *Access Gateway* zukommen, sind zum einen der Aufbau des SSL Tunnels zum Client, bzw. die Verschlüsselung des Datenverkehrs, und zum anderen die Zugriffskontrolle, bei der das Gateway im Grunde genommen wie eine NAT Firewall funktioniert.

SSL-VPNs sind die geeignete Lösung für Remote Access, während bei traditionellen site-to-site Vernetzungen (wie Filialanbindungen etc.) die Verwendung eines IPSec VPNs zu bevorzugen ist. Bei SSL muss nicht, wie bei IPSec, auf jedem Endgerät ein IPSec VPN-Client installiert und konfiguriert werden. Außerdem sind SSL-Sitzungen weniger empfindlich für die im Zusammenhang mit Wählverbindungen oftmals auftretenden instabilen Netzwerkbedingungen (vgl. Sec06a).

Die Kommunikation zwischen Server und Client wird verschlüsselt und damit abgesichert. Das *Access Gateway* kann dafür unterschiedliche Verschlüsselungsalgorithmen verwenden (z.B. RSA, AES 256 Bit, SHA). Der Benutzer meldet sich am *Access Gateway* mit seinem Benutzerschlüssel und Passwort an, um Zugang zu den

für ihn freigegebenen Ressourcen zu erhalten. Dabei ist es möglich, eine Pass-Through Authentifizierung zu benutzen, bei der Benutzerdetails an den *Presentation Server* oder andere Komponenten weitergegeben werden und somit Single Sign-On realisiert werden kann. Eine starke Authentifizierung mittels *SecurID* Karten oder anderer Smart Cards wird ebenfalls unterstützt (vgl. Cit06a). Der Einsatz von *SecureID* Karten wird im Rahmen des Projektes bei Linde in Kapitel 6.4.1 beschrieben.

Der Zugriff des Clients auf das *Access Gateway* erfolgt mit Hilfe eines Browsers. Das dafür benötigte ActiveX Steuerelement wird bei Bedarf automatisch heruntergeladen. Nach dem Login leitet das *Access Gateway* entweder auf das Webinterface, auf eine schon existierende, vorgegebene Standardportalseite oder eine beliebige, sich im Betrieb befindende Unternehmensportalseite um.

Das *Access Gateway* übernimmt dabei die Zugriffskontrolle zu Komponenten und zugänglichen Netzwerken. Es muss mit Hilfe so genannter Netzwerk Ressourcen-gruppen explizit festgelegt werden, auf welche Ressourcen eine Benutzergruppe Zugriff hat. Eine Ressourcengruppe kann z.B. den Zugriff auf eine einzelne Anwendung, eine Gruppe von Anwendungen, einen Bereich von IP-Adressen, ein Subnetz oder das gesamte Intranet beinhalten (vgl. Cit06a).

Die wirkliche Innovation bei der "Access" Strategie von Citrix ist allerdings *Advanced Access Control*, das im Zusammenhang mit dem *Access Gateway* über eine vergleichbare SSL-VPN Lösung von anderen Anbietern hinaus geht. Bei *Advanced Access Control* handelt es sich um ein eigenständiges Produkt, das allerdings nur im Zusammenhang mit dem *Access Gateway* vertrieben wird (siehe Abbildung 3.13). Die Software ist eine Webapplikation, die auf einem IIS Server läuft, und die zwischen dem *Access Gateway* und z.B. dem Webinterface steht.

Der *Advanced Access Control* Server wirkt dabei wie ein Proxy und filtert die Ressourcen, die über den *Presentation Server* angeboten werden. Der eigentliche Clou ist die Endpunkt Analyse, die beim Verbindungsaufbau zum *Access Gateway* durchgeführt wird. Dabei werden Informationen zur Hardware des Clientgeräts, zum Betriebssystem und dessen Updates und Informationen zu Applikationen gesammelt. Es ist z.B. möglich zu erfragen, ob der Client einen aktuellen Virens Scanner auf seinem Rechner laufen hat (vgl. PM06).

Im Zusammenspiel mit dem *Access Gateway* können diese Informationen zur Einteilung des Benutzers in eine Netzwerk Ressourcengruppe genutzt werden, wie beispielsweise "Benutzer von einem firmeneigenen Laptop, außerhalb des Netzwerkes,

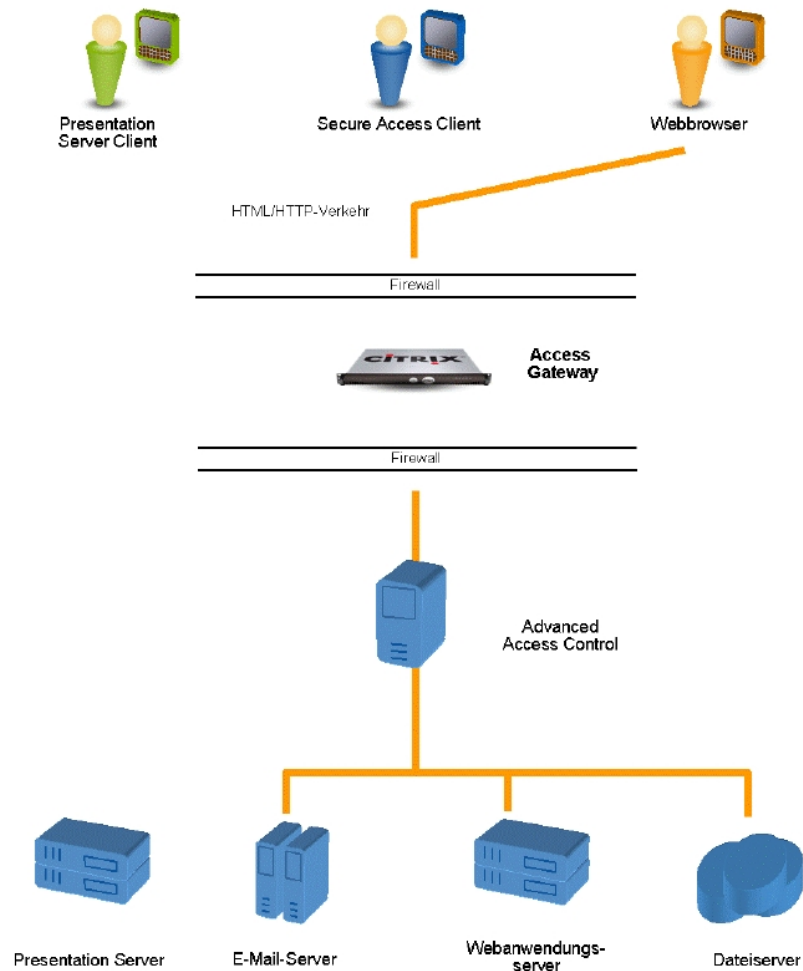


Abb. 3.13: Netzwerkarchitektur mit *Access Gateway* und AAC. Quelle: Citrix

mit funktionierendem Virens Scanner". Auf Grund dieser erstellten Regeln können dann sehr granular Rechte auf Applikationen, Netzwerkressourcen und Daten gegeben werden.

Als weitere Funktion bei *Advanced Access Control* können Administratoren Richtlinien festlegen, die die Anzeige, das Bearbeiten und das Speichern von Dokumenten abhängig von Identität, Gerät, Standort und Verbindung des Benutzers zulassen oder verweigern. Damit können sensitive Daten auch beim Zugriff über das Internet geschützt werden und Vorgaben und Richtlinien im Unternehmen lückenlos als IT Richtlinien durchgesetzt werden (vgl. PM06). Es ist damit z.B. möglich, für nicht vertrauenswürdige Benutzer, eine Excel Datei nur als read-only freizugeben. Diesen Benutzern ist es nicht möglich die Datei zu speichern oder zu bearbeiten. Außer einem Screenshot gibt es keine Möglichkeit Daten der Excel Datei auf dem Clientgerät zu sichern.

Mit *Advanced Access Control* können auch die Sessionparameter angepasst werden. Je nachdem, ob das Clientgerät ein Laptop oder z.B. nur ein Handheld PC mit sehr kleinem Display ist, kann die Bildschirmauflösung oder die Farbtiefe angepasst werden.

Advanced Access Control bietet eine Lösung des Problems, das viele Firmen haben, wenn sich fremde PCs, über die keine Informationen vorliegen, in das Firmennetzwerk verbinden. Das können Mitarbeiter an ihren Rechnern Zuhause oder externe Personen mit ihren PCs sein. Die Sicherheitsrisiken, die dadurch entstehen, wie das Einschleppen von Viren oder das unerlaubte Kopieren von wichtigen Informationen, bereiten vielen Administratoren Kopfschmerzen.

Neben *Advanced Access Control* gibt es noch weitere Lösungen, um einen sicheren Zugang für Fremd PCs zu schaffen. VMWare verfolgt mit der Assured Computing Environment (= ACE) einen Ansatz, bei dem der Administrator ein selbst aufgesetztes Betriebssystem mit allen nötigen Updates und Applikationen in eine abgesicherte virtuelle Umgebung (siehe Kapitel 3.1.1) packt und dieses erstellte Paket an einen nicht überwachten, fremden PC mit Hilfe einer CD oder DVD verteilt (vgl. VMW06a).

Das Paket wird auf dem Client Rechner ausgeführt und der Benutzer hat nur über die virtuelle Umgebung Zugang zu festgelegten Ressourcen (siehe Abbildung 3.14). Der Unterschied zu *Advanced Access Control* ist, dass die Konfiguration des Client Gerätes nicht überprüft wird und anhand des Zustandes des Systems Rechte verge-

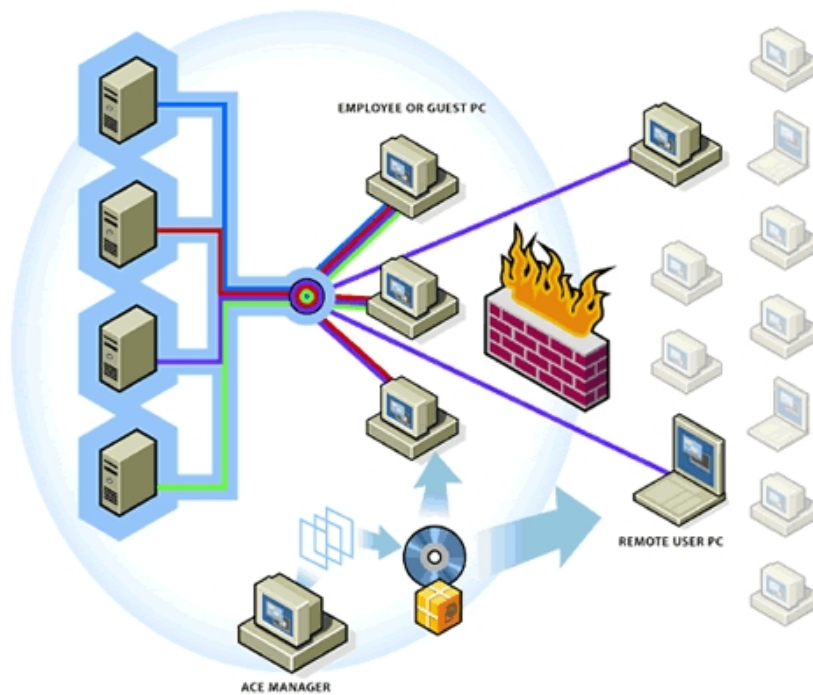


Abb. 3.14: Mit ACE lässt sich der Zugriff von externen Benutzern auf das Netzwerk regeln. Quelle: VMWare



Abb. 3.15: Der Administrator kann bei ACE die genauen Berechtigungen für den Zugriff auf das Netzwerk festlegen. Quelle: VMWare

ben werden, sondern der Administrator die Konfiguration des Systems, von dem auf das Netzwerk zugegriffen wird, selbst bestimmt (vgl. [Mad05b](#)) (siehe Abbildung 3.15).

ACE bietet damit eine noch höhere Sicherheit als *Advanced Access Control*. Es bedeutet aber auch einen höheren Aufwand, da das ACE Paket an jeden fremden Rechner verteilt werden muss, während beim *Advanced Access Control*, sobald das Design der Regeln abgeschlossen und implementiert ist, keine zusätzliche Arbeit bei neuen PCs nötig ist (vgl. [Mad05b](#)).

3.5 Bewertung der Technologien im Überblick

In diesem Kapitel wird noch einmal zusammengefasst, wie sich die vorgestellten Lösungen des Kapitels 2.5 und der Kapitel 3.1, 3.2 und 3.3 im Hinblick auf ausschlaggebende Kriterien verhalten.

Die Gewichtung dieser Kriterien führt letztendlich zur Entscheidung für ein Konzept oder die Mischung mehrerer Konzepte zur Bereitstellung von Applikationen für die Benutzer. In der Abbildung 3.16 sind die Bewertungen zusammengefasst.

	Terminal Services	Personal Computer	Automatische Software-distribution	Streaming	Bladed PC	VDI
Wartungsaufwand	Gering	Sehr hoch	Mittel	Sehr gering	Hoch	Hoch
Aufwand für die Einrichtung eines neuen Arbeitsplatzes	Sehr gering	Sehr hoch	Mittel	Sehr gering	Hoch	Mittel
Wahrscheinlichkeit von Anwendungskonflikten	Hoch	Mittel	Niedrig	Nicht vorhanden	Mittel	Mittel
Zugriff über das Internet	Sehr einfach, Zugriff auf Server	Umständlich, Rechner muss online sein	Umständlich, Rechner muss online sein	Sehr einfach, Zugriff auf Server	Einfach, Zugriff mit RDP auf Blade	Einfach, Zugriff mit RDP auf VDI
Offlinebetrieb	Nein	Ja	Ja	Ja, falls Paket gestreamed wurde	Nein	Nein
Ausfallsicherheit	Von jedem Clientgerät aus nutzbar, aber Server ist single point of failure	Defekter Rechner muss ausgetauscht und neu aufgesetzt werden	Rechner kann schneller neu aufgesetzt werden	Von jedem Clientgerät aus nutzbar, aber Server ist single point of failure	Blade kann einfach ausgetauscht werden	VDI kann auf anderen Rechner verschoben werden
Datensicherheit	Sehr gut (mit AAC)	Schlecht	Schlecht	Mittel	Gut	Gut
Kosten für die Anschaffung	Sehr hoch	Gering	Mittel	Hoch	Hoch	Gering

Abb. 3.16: Vergleich der vorgestellten Lösungen zur Bereitstellung von Applikationen

Kapitel 4

Ausblick

Im Moment befindet sich der Markt für Terminal Services und Server Based Computing in einer Umbruchphase. Ähnlich wie mit der Veröffentlichung von Windows Server 2000 oder Windows Server 2003, werden mit der Veröffentlichung von Windows *Vista* bzw. der Server Version *Longhorn* die Rahmenbedingungen neu gesteckt. Im Kapitel 4.1 werden die Neuerungen für Terminal Services in der neuen Windows Server Version vorgestellt und die Auswirkungen auf Zusatzanbieter wie Citrix beleuchtet.

Das neue Windows wird eine neue Präsentationsschicht enthalten, die auf lange Sicht die Art, wie Terminal Server arbeiten, komplett verändern könnte (siehe Kapitel 4.2). Da Anbieter wie Citrix immer mehr unter Druck geraten und neue Funktionalitäten in ihre Produkte integrieren müssen, die einen Kauf rechtfertigen, wird in Kapitel 4.3 der Kauf von Reflectent durch Citrix analysiert, und welche Chancen Performance Measuring in Terminal Server Umgebungen bringen kann.

4.1 Mircosoft Longhorn Server

Schon 2003 machten Gerüchte die Runde, dass Microsoft unter dem Codenamen "Bear Paw" wichtige Neuerungen am Terminal Server vornehmen will. Der Zeitplan verzögerte sich allerdings immer weiter nach hinten. Erst sollten die neuen Funktionalitäten in einem Servicepack für Windows Server enthalten sein, dann in dem zweiten Release von Windows Server 2003 Anfang diesen Jahres. Nun sieht es so

aus, als würde erst im nächsten Jahr mit der Veröffentlichung des *Longhorn Servers* der Terminal Server erweitert werden (vgl. [Mad04b](#)).

Im Grunde genommen wird Microsoft die meisten und wichtigsten Zusatzfunktionen der Citrix Produkte in den Terminal Server integrieren. Die vollständige Liste der neuen Funktionen umfasst (vgl. [Mad03b](#)):

- Publizieren von Anwendungen und die nahtlose Integration, wie z.B. Einträge ins Startmenü, Registrierung der Dateitypen usw.
- Seamless Window: Anwendungen müssen nicht mehr in einer Remote Desktop Umgebung gestartet werden, sondern erscheinen als würden sie lokal gestartet
- RDP kann verschlüsselt über HTTPS übertragen werden und bietet damit eine ähnliche Funktionalität wie das Citrix Access Gateway
- Ein Webinterface wird enthalten sein, durch das der Zugang zu einzelnen Applikationen ohne den Start eines kompletten Remote Desktops möglich ist
- Die neue Version von RDP in der Version 6 bietet Verbesserungen im Bandbreitenbedarf und in der Konfiguration von virtuellen Kanälen
- Verbesserungen bei Benutzer Profilen und der Lizenzierung

Das macht deutlich, dass Microsoft damit die meisten Funktionalitäten, die bisher den Ausschlag für den Einsatz von Citrix gegeben haben, im Terminal Server integriert. Die beiden Punkte, die nicht in Angriff genommen wurden, sind das Load Balancing der Serverfarm und das Verwalten von Sessions mit zusätzlichen Session Directories.

Mit dem Release von *Longhorn Server* wird es zunehmend auch für mittlere und große Unternehmen interessant, eine reine Terminal Server Lösung ohne Zusatzanbieter zu wählen. Insgesamt wird die Attraktivität des Terminal Servers noch einmal gesteigert, womit sich die positive Entwicklung der letzten Jahre fortsetzen dürfte.

Für Citrix und andere Zusatzanbieter brechen damit schwere Zeiten an. Auch wenn Citrix z.B. mit dem angekündigten *Project Constellation*, das genauer im Kapitel [4.3](#) besprochen wird, weiterhin versucht, das Terminal Server Basisprodukt zu verbessern, wird es doch immer schwieriger, Kaufanreize zu kreieren. Von der fast allumfassenden Marktdominanz bei Terminal Services der letzten Jahre wird sich

Citrix wohl verabschieden und den Weg in neue Märkte weiter vorantreiben müssen (vgl. [Mad03c](#)).

4.2 Microsoft Vista Presentation Layer

Eine weitere interessante Verbesserung im neuen Windows Betriebssystem ist die neue Präsentationsschicht mit dem Namen Windows Presentation Foundation (= WPF), die früher unter dem Codenamen "Avalon" angekündigt wurde.

Die WPF ist Teil der auf .NET basierenden Klassenbibliotheken WinFX (= Windows Framework), die als Programmierschnittstelle für das neue Betriebssystem vorgesehen sind (vgl. [Sch06c](#)).

Während die Funktionalität von WPF bestätigt ist und es auch schon eine Veröffentlichung von WinFX gibt, kann über die Auswirkung der Einführung dieses Frameworks zur Entwicklung grafischer Benutzerschnittstellen, besonders auf Terminal Services, nur spekuliert werden.

Mit WPF kann die Windowsoberfläche durch eine auf XML basierende Sprache beschrieben werden. Microsoft nennt diese Erweiterung XAML (= Extensible Application Markup Language), mit der Objekte zur Anzeige wie Buttons, Formulare, Toolbars oder Medienelemente in XAML Tags definiert werden (vgl. [Sch06c](#)).

Beispiel für die XAML Syntax:

```
<Window Text="Beispiel für XAML">
  <FlowPanel>
    <SimpleText>Textbox mit Buttons</SimpleText>
    <TextBox ID="ValueTextBox" HorizontalAlignment="Center"
      IsReadOnly="True"/>
    <FlowPanel HorizontalAlignment="Center" Width="100%">
      <Button Click="Dec">Dec (-)</Button>
      <Button Click="Clear">Clear</Button>
      <Button Click="Inc">Inc (+)</Button>
    </FlowPanel>
  </FlowPanel>
</Window>
```

Einen WinFX Client vorausgesetzt, zeichnet der Rechner anhand der XAML Beschreibung den Bildschirminhalt auf den Monitor. Der für Terminal Services interessante Fall ist das Erstellen von XAML Beschreibungen auf dem Server und das

eigentliche Anzeigen des Bildschirms auf dem Client. Die Bildschirmausgabe muss also nicht mehr auf dem Server in ein Bildformat gespeichert und komprimiert werden und über ein Präsentationsprotokoll zum Client übertragen werden, sondern der Server schickt dem Client eine Beschreibung des Inhalts in Form einer XAML Datei.

Neben der geringeren Rechenleistung auf dem Server und der Reduzierung der Bandbreite, kann mit WinFX auch sichergestellt werden, dass die Applikation das Erscheinungsbild bzw. Look-and-Feel des Clients hat, da der Client die XAML Befehle selbst interpretiert.

Insgesamt ist die Funktionsweise von WPF ähnlich der von HTML, denn der Server schickt eine Beschreibung des Inhalts an den Client, der diese selbstständig verwertet. Mit XAML ist es theoretisch auch möglich Anwendungen im Internet zu benutzen, die auf dem Client wie native Programme wirken, denn XAML zeichnet im Gegensatz zu HTML nicht nur in den Browser, sondern kann nahezu alle Instanzen des Betriebssystems zur Anzeige beschreiben (vgl. [Sch06a](#)).

Es bleibt abzuwarten, wie groß der Erfolg von XAML ausfallen wird, doch steht damit eine mächtige Konkurrenztechnologie zu traditionellen HTML Webseiten in den Startlöchern. Für den Terminal Server ist anzumerken, dass sich, bei einer Unterstützung von XAML, die Funktionalität an die eines Web Servers in gewissem Maße angleicht. Während der Web Server für eine Web Applikation HTML zum Client schickt, sendet der Terminal Server die Bildschirminhalte einer nativen Applikation per XAML zum Client (vgl. [Mad06b](#)).

Microsoft hat bereits angekündigt, dass es möglich sein wird, beim neuen *Longhorn* Terminal Server zu erfragen, ob ein Client WinFX- fähig ist und je nachdem XAML an den Client zu schicken bzw. auf dem traditionellen Weg den Bildschirminhalt auf dem Server zu rendern und als Screenshot mit RDP zu versenden (vgl. [Mad03b](#)). Es wird sich zeigen, wie viele Anwendungen in Zukunft XAML fähig sein werden, und ob sich diese Technologie durchsetzen wird.

4.3 Performance Measuring und Traffic Shaping

Anfang Mai 2006 übernahm Citrix mit Reflectent einen Anbieter für Application Performance Monitoring Software (vgl. [Cit06c](#)). Zusammen mit dem Kauf von Netscaler Mitte des Jahres 2005, die Netzwerk Hardware zum Load Balancing und zur Opti-

mierung des Datenverkehrs im Portfolio hatten (vgl. Cit05), lässt Citrix den Weg, der in den nächsten Jahren vermutlich eingeschlagen wird, erkennen.

Inzwischen hat Citrix das ehemalige Netscaler Produkt zur Optimierung des Datenverkehrs von Webseiten in das eigene Produktangebot integriert. Diese Lösung wird von bekannten Firmen wie Amazon, Google oder MSN eingesetzt (vgl. Mad05c) und bietet, neben einer verbesserten Routingtechnik, eine Kompression der Daten, optimiertes Load Balancing und SSL Beschleunigung (vgl. Cit05).

Damit drängt Citrix neben dem Angebot des *Access Gateways* (siehe Kapitel 3.4) weiter auf den von Cisco und anderen Anbietern dominierten Markt für Netzwerk Hardware. Während die traditionellen Anbieter früher klassische Switches herstellten und nun, wenn das OSI Schichtenmodell betrachtet wird, auch die Applikationsschicht bedienen, geht Citrix den umgekehrten Weg von den Applikationen hin zu den niedrigeren Schichten. Für welche Lösung sich ein Unternehmen entscheidet, liegt meistens an dessen Ausgangssituation. Falls das Unternehmen schon eine Infrastruktur mit Citrix *Presentation Server* hat, wird auch der Widerstand gegen Citrix Hardware Lösungen geringer sein. Bei Netzwerk Administratoren, die schon immer auf Lösungen von z.B. Cisco gesetzt haben, wird es für Citrix schwer die entsprechende Überzeugungsarbeit zu leisten und sich als Anbieter von Hardwarelösungen zu etablieren (vgl. Mad06b).

Aber auch für das gewohnte Terminal Services Geschäftsfeld mit dem *Presentation Server* werden sich durch die Übernahmen voraussichtlich Änderungen ergeben. Ein gravierender Schwachpunkt des Microsoft Terminal Servers ist das Load Balancing, das nur anhand von Daten zur Netzwerkauslastung betrieben wird. Nun sagt ein viel benutztes Netzwerk noch nichts über den Zustand der Terminal Server aus, deshalb können beim *Presentation Server* Daten zur Anzahl der Benutzer und der Auslastung der CPU des Servers verwendet werden.

Doch selbst das ist meistens nicht sonderlich aussagekräftig. Denn obwohl viele Benutzer auf einem Server arbeiten und die Auslastung hoch erscheint, kann die Benutzung der Anwendungen immer noch ohne Probleme verlaufen. Als umgekehrten Fall kann aber auch ein Benutzer mit einer speziellen, rechenintensiven Anwendung den wenigen anderen Benutzern auf dem Server das Arbeiten unmöglich machen.

Für einen intelligenten Load Balancing Algorithmus sollte also nicht auf die Serverseite geschaut werden, sondern lieber an Hand der Performanz der Benutzer Sessions eine Entscheidung gefällt werden, ob der Server überlastet ist oder nicht (vgl. Cit06c). Die Software von Reflectent misst Parameter der Session, wie z.B die Reaktionszeit, und sammelt Daten vom Client Rechner. Es können Regeln festgelegt werden wie "Server gilt als überlastet, wenn das Öffnen einer Mail in Outlook länger als 20 Sekunden dauert". Zusätzlich hilft das Sammeln der Daten bei der Lösung von Problemen. Wenn sich ein Benutzer beim Help Desk meldet und sich über eine schlechte Verbindung beklagt, kann festgestellt werden, ob der Grund dafür am Server oder am Rechner des Clients (z.B. eine Vielzahl an gleichzeitigen Downloads) zu suchen ist (vgl. Mad06a).

Citrix könnte dieses Konzept mit dem ICA Protokoll umsetzen. Dabei würden Daten des Benutzers über einen virtuellen ICA Kanal an den Server übermittelt oder Daten aus der ICA Session zur Entscheidung beim Load Balancing herangezogen. Zusätzlich könnte die Performanz der einzelnen Benutzersessions mit Hilfe des Know How über Traffic Shaping von NetScaler verbessert werden. Beim Traffic Shaping werden den unterschiedlichen Arten von Traffic verschiedene Prioritäten bei der Weiterleitung zugeordnet. Bei einer ICA Verbindung könnte das z.B. bedeuten, dass der virtuelle Kanal für Druckaufträge eine geringe Priorität erhält, während Tastatur- und Mauskommandos die höchste Priorität erhalten.

Diese und weitere Erweiterungen der Funktionalität, wie die verbesserte Komprimierung und Übertragung von z.B. CAD Dateien, kündigte Citrix unter dem Namen "Project Constellation" an (vgl. Cit06d). Dazu gehört auch das in Kapitel 3.3 erwähnte Streaming Projekt Tarpon. Damit wird folgende Nachricht vermittelt: Egal ob ein Unternehmen Applikationen zentral auf einem Terminal Server, dezentral auf den Rechnern der Benutzer oder als Webapplikation bereitstellen will, Citrix unterstützt mit dem *Presentation Server*, Application Streaming und dem Netscaler Produkt alle drei Ansätze (vgl. Mad05a).

Ob sich Citrix damit gegen Konkurrenz wie Microsoft, die bald mit dem verbesserten Terminal Server und dem SMS mit Streaming Funktionalität auf den Markt gehen wird, durchsetzen kann, bleibt abzuwarten. Den Kunden stehen jedenfalls mehrere gut funktionierende Technologien zur Bereitstellung von Applikationen für ihre Benutzer zur Verfügung. Ob sie den traditionellen Weg mit einer Installation auf Desktop PCs gehen oder Terminal Server, automatische Softwaredistribution mit

oder ohne Streaming, virtuelle Desktops oder Bladed PCs verwenden, entscheidet sich nach einer Analyse und Abwägung der Kriterien im Unternehmen.

Kapitel 5

Die Firma Linde

Der praktische Teil der Arbeit wurde anhand eines Projektes bei der Linde AG, im Geschäftsbereich Engineering, in der Abteilung "Informatik für Verfahrenstechnik" (IV) durchgeführt. Die Abteilung ist im Bereich Informatik angesiedelt, wobei der Schwerpunkt auf Applikationen für die Verfahrenstechnik liegt.

Dieses Kapitel stellt die Firma und die Abteilung mit Aufgabenbeschreibung vor, um ein besseres Verständnis zur Einordnung des Projektes im Konzern zu vermitteln.

5.1 Der Konzern

Linde ist ein internationaler Technologiekonzern, der in seinen beiden Unternehmensbereichen Gas und Engineering sowie Material Handling jeweils führende Marktpositionen besetzt. Mit weltweit rund 42.000 Mitarbeitern erzielt Linde einen Jahresumsatz von 9,501 Milliarden Euro.

Bereits 1879 gründete Carl von Linde (geboren 1842) mit Finanzpartnern in Wiesbaden die Gesellschaft für Linde's Eismaschinen als Aktiengesellschaft.

Als Pionier der Kältetechnik baute er ein dynamisches Unternehmen auf, das sich in den Jahrzehnten unter seiner Leitung zu einem führenden Apparatebauer, Kühlhausbetreiber und Gasproduzenten entwickelte. Früh erfolgte eine internationale Ausrichtung.

1887 erreichte Carl von Linde die Verflüssigung von atmosphärischer Luft, im gleichen Jahr erhielt er das Patent auf sein Verfahren. 1902 gelang nach mehrjährigen

Versuchsarbeiten in Höllriegelskreuth bei München die Herstellung von Sauerstoff durch Luftzerlegung nach dem so genannten Rektifikationsverfahren (vgl. [Lin05c](#)).

Der Anlagenbau wuchs in Höllriegelskreuth ab den 50er Jahren in völlig neue Dimensionen. 1965 wurde die Firma in eine Aktiengesellschaft, die Linde AG, umgewandelt. Für Linde bedeuteten diese Aufträge den Einstieg in den Großanlagenbau mit völlig neuen technischen und finanziellen Herausforderungen.

Zwischen 1980 und 1997 hat sich der Umsatz unter der Leitung des Vorstandsvorsitzenden Dr. Hans Meinhardt von 2,74 Milliarden DM auf 9,55 Milliarden DM mehr als verdreifacht, die Gewinne haben sich nahezu versechsfacht.

Die umfangreiche Geschichte der Erfindungen von Carl von Linde und der Entwicklung des Konzerns ist als Buch mit dem Titel "Die Linde AG: Geschichte eines Technologiekonzerns 1879-2004" im Verlag C.H. Beck erschienen (vgl. [C.H05](#)).

Seit 2002 ist Dr. Ing. Wolfgang Reitzle Vorstandsvorsitzender, der mit verschiedenen Maßnahmen die Linde AG in allen Geschäftsbereichen zu einem führenden Player auf den globalen Märkten machen will.

Im Frühjahr 2004 wurde die Kältetechnik an das US-Unternehmen Carrier Corporation veräußert. Auch nach 125 Jahren besitzt die Linde AG in ihren Unternehmensbereichen Gas, Engineering (Anlagenbau) sowie Material Handling jeweils führende Marktpositionen (vgl. [Lin05b](#)).

Nach der Zustimmung der Eigentümer, wird der englische Gaskonzern BOC voraussichtlich ab 6. September 2006 von Linde übernommen. Damit bilden beide Firmen gemeinsam, mit über 53.000 Mitarbeitern im Gase- und Anlagenbaugeschäft in mehr als 70 Ländern, sowie mit einem Umsatz von zwölf Milliarden Euro, das weltweit führende Industriegaseunternehmen.

5.2 Linde Engineering

Der Geschäftsbereich Linde Engineering umfasst den Anlagenbau. Verfahrenstechnische Anlagen zählen zu den größten und kompliziertesten Bauwerken der Menschheit. Linde zählt mit mehr als 1.500 verfahrenstechnischen Patenten und 3.500 gebauten Anlagen zur Weltspitze. In diesem Segment plant und baut Linde schlüsselfertige Industrieanlagen für verfahrenstechnische Projekte.

Linde Engineering bietet Ingenieurberatung, Projektmanagement, Planung und

Kontrolle von Terminen, Kapazitäten und Kosten, verfahrens- und ingenieurtechnische Auslegung, Beschaffung, Bau, Montage und Inbetriebnahme sowie Personalschulung und Kundendienst als Dienstleistungen (vgl. [Lin05a](#)).

Diese Leistungen werden für viele unterschiedliche Arten von Anlagen erbracht, u.a. für:

- Chemie- und Petrochemie-Anlagen: u.a. Gewinnung von Ethylen, Propylen, Acetylen, Butadien, Benzin (siehe Abbildung [5.1](#))
- Wasserstoff- und Synthesegas-Anlagen: u.a. Erzeugung von Wasserstoff, Kohlenmonoxid und Mischungen dieser beiden Gase (Synthesegas)
- Gasaufbereitungsanlagen: Reinigung und Trennung von Gasgemischen
- Erdgasaufbereitung: u.a. Aufbereitung und Konditionierung von Rohgas zu Heizgas
- Luftzerlegungsanlagen: u.a. Verfahren zur Verflüssigung von Atmosphärenluft und sonstigen Gasen
- Kryotechnische Anlagen: Erzeugung tiefster Temperaturen
- Umwelthanlagen: Lösungen für spezifische Aufgabenstellungen in den Arbeitsgebieten Abfallbehandlung, Abwasserreinigung, Wasseraufbereitung und Abgas-/Abluftreinigung

Hauptsitz des Geschäftsbereichs Linde Engineering ist Pullach bei München. Wichtige Standorte sind die Linde-KCA-Dresden GmbH, einer der Marktführer bei Pharmazie- und Umweltschutzanlagen, die Sela-Linde GmbH, Pullach, die auf Industrieöfen und Verbrennungsanlagen spezialisiert ist, sowie zahlreiche ausländische Konzerngesellschaften und Vertriebsbüros.

5.3 Der Bereich Informatik

Der Bereich Informatik (I) ist verantwortlich für die Bereitstellung von IT Applikationen, welche für das operative Geschäft bei Linde Engineering benötigt werden. Hier werden Anwendungen geplant, entwickelt und gepflegt, während das Data Center Munich als Teil der Linde IT Services (LIS) u.a. für die IT-Infrastruktur, für das Help Desk und für den Betrieb des Netzwerks und der Server zuständig ist.



Abb. 5.1: Beispiel einer Chemie/Petrochemie Anlage. Quelle:Linde

Innerhalb des Bereichs I sind die Abteilungen IA ("Informatik für Administration und kaufmännische Projektabwicklung"), IE ("Informatik für Ingenieurtechnik") und IV ("Informatik für Verfahrenstechnik") für die Bereitstellung von IT-Applikationen verantwortlich, welche jeweils unterschiedlichen Zwecken bei Linde Engineering dienen.

Die Leitung des Bereichs I koordiniert die Anforderungen von Linde Engineering im Rahmen der Informatik Strategie und setzt u.a. Prioritäten bei der Zuordnung von Ressourcen.

5.4 Abteilung "Informatik für Verfahrenstechnik"

Die Abteilung "Informatik für Verfahrenstechnik" (IV) ist zuständig für die Bereitstellung von IT-Applikationen für die Unterstützung der Abläufe im Prozess Design, in der Stoffdatenberechnung und bei der Prozessführung bei Linde Engineering.

Im einzelnen sind das folgende Abläufe(vgl. [Lin02](#)).

- Anlagenauslegung mit Prozess-Simulatoren
- Stationäre und dynamische Anlagensimulation und -optimierung
- Stoffdatenberechnung im Rahmen der Anlagen- und Apparateauslegung (Verfahrensrechnung)

- Speicherung und Dokumentation der verfahrenstechnischen Daten/Ergebnisse
- Kinetische Rechnung der Ethylenspaltöfen
- Simulation und Optimierung ausgewählter Apparate (Wärmetauscher, Kompressoren)
- Entwicklung und Anwendung von Methoden und Konzepten für Prozessführung beim Anlagenbetrieb
- Bereitstellung von Systemen für Operatorschulung und Betriebsoptimierung
- Lösung verschiedener mathematischer Problemstellungen

In der Abteilung werden in Absprache mit den anwendenden Fachbereichen, Töchtern und Partnern Programme und Systeme zur verfahrenstechnischen Berechnung und Simulation beim Anlagenbau erstellt und zur Verfügung gestellt. Die Programme dienen im wesentlichen der verfahrenstechnischen Auslegung der Anlagen, d.h. dem Prozess Design. Dabei kommen vor allem Eigenentwicklungen zum Einsatz, welche einen bedeutenden Anteil an schützenswertem Know How beinhalten. Daneben gibt es kommerzielle Programme, die in der Regel mit internen Entwicklungen gekoppelt werden.

Eine wichtige Applikation ist z.B. der Linde-interne Prozess Simulator *OPTISIM*, mit dem Simulationen von verfahrenstechnischen Prozesse durchgeführt werden können, um diese Prozesse zu bewerten und zu optimieren.

Details zum Prozess Design und *OPTISIM* sind nachzulesen bei (Bur91), (KESL97) und (EK06).

Das in den folgenden Kapiteln beschriebene Projekt beinhaltet die Bereitstellung dieser bei der IV vorhandenen Applikationen über eine webbasierende Portallösung.

Kapitel 6

Prozess Design Portal

Für den praktischen Teil der Arbeit wurde bei Linde Engineering im Rahmen eines Projektes ein Portal zur Zusammenführung von Applikationen und Informationen erstellt. Dabei wird an einem konkreten Beispiel der Einsatz einer Terminal Service Umgebung in einem Unternehmen vorgestellt.

Nach einer Kurzbeschreibung wird auf die Anforderungen (vgl. Kapitel 6.2) und Ziele (vgl. Kapitel 6.3) des Projektes eingegangen. Für die Arbeit besonders von Bedeutung ist dabei die getroffene Entscheidung der Beibehaltung der Citrix Umgebung (vgl. Kapitel 6.4.1), sowie die in Kapitel 6.5 beschriebene Umsetzung mit der Einrichtung des Webinterfaces und der Integration in das Portal.

6.1 Kurzbeschreibung

Für Linde Engineering in Pullach wird eine geeignete, webbasierende Umgebung zur Versorgung von Benutzern außerhalb des Standortes Pullach mit Applikationen und Informationen zum Prozess Design (Auslegung der Anlagen bzw. verfahrenstechnische Prozesse) erstellt.

Nach einer Analyse der Rahmenbedingungen und der Ausgangssituation, wie z.B. der Bewertung der aktuell betriebenen Citrix Lösung, werden Alternativen und deren Potenziale bei einer Umsetzung aufgezeigt.

Dabei ist absehbar, dass sich sowohl der Kreis der externen Nutzer, als auch das Angebot an Applikationen gegenüber dem aktuellen Stand deutlich ausweiten wird. Damit einhergehend soll die Effizienz hinsichtlich Verwaltung, Benutzerservice und Konfigurationsmanagement gesteigert werden. Eine benutzerfreundliche, persona-

lisierte Oberfläche soll einen Werbeeffect erzeugen und weitere Anwender für die Werkzeuge gewinnen.

Auf diesem Weg wird u.a. die Produktivität aller neuen Anwender gefördert. Der Know How Schutz wird überprüft und bei Bedarf optimiert. Im Zusammenhang mit dem Projekt sind auch für eventuelle zukünftige Vorhaben neue, nutzbare Technologien zu erkunden.

Für den Administrator wird die Transparenz sowohl im Hinblick auf zugelassene Benutzer und ihre Berechtigungen als auch auf Applikationen und zugehörige Informationen inklusive zugehöriger Versionsstände verbessert.

6.2 Funktionalität

Das Prozess Design Portal ist eine webbasierte Plattform für Töchter, Partner und Mitarbeiter auf Reisen, die Applikationen über das WAN bereit stellt. Die damit zusätzlich verbundenen Informationen wie Benutzerhandbücher, benötigte Dateien, Links u.ä. werden mit den Anwendungen an einer zentralen Stelle gebündelt.

Beim aktuellen bisherigen Szenario wählen sich die Töchter und Partner per VPN in das Linde Netzwerk ein und haben mit Hilfe der *Program Neighborhood* Software Zugriff auf die für sie freigegebenen Applikationen. Die Zusatzinformationen sind auf Netzwerklaufwerken oder im Intranet verteilt oder sie werden per Email gesondert verschickt.

Im neuen Portal werden wichtige Applikationen der Abteilung IV, wie z.B. *OPTISIM* oder *PC VIPS*, unterstützt. Zusätzlich sind auf der Webseite Listen von Stoffdaten einsehbar und filterbar. Stoffdaten werden für die Simulationen und Berechnungen benötigt und sind bisher für interne und externe Mitarbeiter nur umständlich aufrufbar.

Wichtig ist die flexible Erweiterbarkeit der Plattform. Es können zusätzliche Anwendungen und nahezu alle Arten von Content eingebunden werden, um für zukünftige Entwicklungen gewappnet zu sein. Neben Links ins Internet und Intranet, werden auch alle gängigen Dateiformate (Acrobat, Microsoft Office usw.) unterstützt.

Benutzer haben nur Zugriff auf die für sie freigeschalteten Applikationen und Informationen. Da es mehrere Gruppen mit unterschiedlichen Profilen gibt, muss es eine granulare Rechtevergabe für Anwendungen und Dokumente geben.

Bei einigen Applikationen muss der bestehende Lizenzschutz gewahrt bleiben und unerlaubtes Kopieren von sensiblen Daten muss unterbunden werden. Das gilt zum einen für die Dokumente selbst, zum anderen aber auch für den Inhalt einiger Dokumente, der mit Kopierschutzmechanismen geschützt werden muss.

Die Benutzer- und Rechteverwaltung soll für den Administrator vereinfacht werden. Da die Vergabe von Rechten auf unterschiedliche Ebenen und Systeme verteilt ist, ist es wünschenswert, dass die Einsicht und Verwaltung von Rechten auf nur einer Plattform, dem Portal, möglich ist.

Das Portal wird auch den Support und die Genehmigungsworkflows vereinfachen, indem Ansprechpartner mit Kontaktinformationen genannt werden. Z.B. werden Benutzer sofort erkennen können, wen sie im Falle eines Anwendungsfehlers kontaktieren können bzw. wer Rechte für bestimmte Ressourcen vergeben kann.

6.3 Ziele

Ein wichtiges Ziel des Projektes ist das Aufzeigen von Alternativen für die Erstellung eines solchen Portals. Auf die Bewertung der Citrix Umgebung und die Auswahl zwischen einer normalen Webapplikation und einer Lösung mit einem Portalserver wird in den Kapiteln 6.4.1 bzw. 6.4.2 und 6.4.3 eingegangen. Wesentlich war ein Vergleich zwischen Aufwand und Nutzen und das Aufzeigen der Potenziale der einzelnen Lösungen.

Des wesentliche Ziel des Projekts ist die Umsetzung der vorgeschlagenen Lösung. Mit dem Portal werden im Detail die folgenden Ziele verfolgt:

Durch vereinfachte Nutzung und die Bündelung von Informationen und Applikationen für effizienteres Arbeiten, soll der externe Nutzerkreis erweitert bzw. Töchtern von Linde stärker eingebunden werden.

Mitarbeitern soll es durch die Webbasiertheit der Lösung möglich sein, von jedem Standort aus, über das Internet auf die Plattform zugreifen zu können.

Der Benutzerservice soll verbessert werden, indem eine einfach zu bedienende

Seite zur Verfügung gestellt wird und benötigte Kontaktinformationen bei Problemen mit den Anwendungen oder mit dem Portal leicht zu finden sind.

Der Administrator der Seite soll durch eine vereinfachte, zentrale Verwaltung von Benutzern, Applikationen und Dokumenten inklusive Rechtemanagement entlastet werden. Es ist das Ziel, Updates und neue Releases schneller und mit wenig Aufwand an die betroffenen Nutzer zu verteilen.

Die Transparenz hinsichtlich der Rechtevergabe für den Zugang zu Applikationen und Dokumenten soll verbessert werden und der Versionsstand von Applikationen leichter erkennbar sein.

Durch einen geeigneten Know How Schutz soll das Eigentum von Linde Engineering weiterhin zuverlässig vor Missbrauch geschützt werden. Alternativen zum bisherigen Know How Schutz sind zu prüfen.

Insgesamt soll durch die Erstellung des Prozess Design Portals die innovative Kompetenz der Abteilung IV gestärkt werden.

6.4 Technologieauswahl

6.4.1 Citrixumgebung

Ein Kernstück des Prozess Design Portals ist die Bereitstellung von Applikationen der Abteilung IV. Bei der Analyse der Ausgangssituation und der Rahmenbedingungen wurde schnell klar, dass eine Beibehaltung der verwendeten Citrix Infrastruktur viele der Anforderungen ohne zusätzlichen Aufwand lösen würde.

In der Ausgangssituation hat sich ein Mitarbeiter eines anderen Standortes, wie z.B. der LBPP (Linde BOC Process Plants) in den USA, in das interne Netzwerk per VPN eingewählt und hat die *Program Neighborhood* Software auf seinem Rechner gestartet, um sich mit dem *Presentation Server* zu verbinden.

Linde verfügt über die Lizenz für die Citrix *Access Suite 4.0* mit dem enthaltenen *Presentation Server*, dem Webinterface und der SSL-VPN Lösung *Access Gateway*. Damit gibt es bei Linde Ansprechpartner, die bereits viel Erfahrung mit Citrix haben. Eine Terminal Service Lösung ist auch im Einklang mit der langfristig ausgelegten

Strategie, bei Linde Applikationen für mobile Nutzer über Citrix bereit zu stellen und hat somit die garantierte Akzeptanz durch z.B. das Data Center.

Die für die IV wichtigen Applikationen waren bereits auf dem *Presentation Server* installiert und für bestimmte Gruppen freigegeben. Die Migration der Anwendungen auf den Server entfiel somit in vielen Fällen und auch für eine Absicherung durch Rechtevergaben an einzelne Windowsgruppen war bereits gesorgt.

Die zwei wichtigsten Gründe für eine Beibehaltung des Zugangs über Citrix waren zum einen die Abdeckung der Anforderungen des Projekts und zum anderen der Mangel an Alternativen zu Terminal Services bzw. zum Server Based Computing.

Wie im Kapitel 2.6.2 beschrieben, kann mit Hilfe des Citrix Webinterfaces auf publizierte Anwendungen über das Internet zugegriffen werden. Im Endeffekt wird damit eine webbasierte *Program Neighborhood* zur Verfügung gestellt.

Die Anwendungen von Linde sollen nur von berechtigten Benutzern verwendet werden. Bei einer Terminal Service Lösung verlässt die Software nicht das Haus, kann aber von Externen benutzt werden. Das Szenario mit Vor- und Nachteilen wurde bereits im Kapitel 2.6.3 besprochen.

Die Rechte für den Zugriff können leicht mit Einstellungen beim *Presentation Server* verwaltet werden. Es ist eine Anbindung an das Active Directory von Windows möglich und es können existierende Gruppen zur Regelung verwendet werden. Auf der Benutzerseite kommen nur Bildschirminhalte an, während die eigentliche Programmlogik bzw. die Sourcen des Programms komplett verborgen bleiben. Durch die bereits bestehende Anbindung von z.B. *OPTISIM* an einen Lizenzserver kann zusätzlich noch sicher gestellt werden, dass der Benutzer im Besitz einer Lizenz für die Anwendung ist. Damit war die Anforderung nach Wissensschutz nahezu komplett abgedeckt. Der Contentschutz z.B. einer Excel Tabelle kann wie in Kapitel 3.4 durch *Advanced Access Control* und der Ausweisung des Contents auf "Read only" erreicht werden.

Der Mangel an Alternativen bekräftigte den Entschluss für eine Citrix Umgebung. Die Programme wurden über Jahre hinweg nativ programmiert. Eine Umstellung auf Web Services hätte zu viel Zeit in Anspruch genommen. Da die Software nicht außer Haus gegeben werden sollte, d.h. keine vollwertigen Kopien verteilt werden sollten, kam auch keine Software für automatische Softwaredistribution wie SMS (vgl. 2.5.3) oder Streaming mit *Softgrid* (vgl. 3.3) in Frage. Neue Ansätze wie virtuelle Desktops und Bladed PCs sind noch nicht am Markt etabliert und bei Linde gibt es damit

noch keine Erfahrungen. Terminal Services sind die geeignetste Möglichkeit native Programme über das WAN zur Verfügung zu stellen, ohne die Programmdateien in irgendeiner Form auf die Clients zu kopieren.

Durch die Entscheidung für Citrix ergab sich die Möglichkeit mit dem Webinterface die fehlende Webfähigkeit in der alten Lösung zu beheben. Im alten Szenario konnten sich die Benutzer nur von bestimmten Standorten, deren IP Adressen freigeschaltet waren, zum Linde Netzwerk verbinden. Das schloss Benutzer außerhalb ihres Arbeitsplatzes, z.B. auf Reisen, aus.

Das Data Center verweigerte im Rahmen der Umstellung bei Linde auf SSL-VPN das Freischalten von IP Adressen für neue Standorte. Deshalb musste, um das angestrebte Ziel, eine Erweiterung des Nutzerkreises zu schaffen, zu erreichen, der Zugang zum Prozess Design Portal mit der SSL-VPN Strategie in Einklang gebracht werden.

Die Benutzer können sich nach der Einführung von SSL-VPN nur noch mit einer *SecurID* Karte, bzw. starken Authentifizierung im Firmennetzwerk anmelden. *SecurID* ist ein Sicherheitssystem zur Authentifizierung von Benutzern der Firma RSA Security. Die Authentifizierung ist eine Zweifaktor-Authentifizierung, durch die eine hohe Sicherheit gewährleistet werden soll. Der Benutzer muss ein persönliches Kennwort festlegen und im Besitz seines Tokens bzw. der *SecurID* Karte sein. Der Token generiert jede Minute eine neue Zahl, die durch den Server validiert werden kann (vgl. [Sec06b](#)). Eine gültige Zahlenfolge kann nur mit Hilfe des Tokens generiert werden.

Für den Betrieb der Seite ergibt sich dadurch, dass Standorte, die bereits durch ihre IP Adresse freigeschaltet sind, sich auch ohne *SecurID* Karte in das Firmennetzwerk verbinden können. Dagegen müssen neue Standorte und Mitarbeiter auf Reisen eine *SecurID* Karte beantragen, um Zugang zum Netzwerk bzw. zum Prozess Design Portal zu erhalten.

Bei IV-internen Diskussionen kam der Vorschlag auf, auch bei internen Mitarbeitern in Zukunft Anwendungen über das Portal, anstatt als lokale Installation zu starten. Da dieser Personenkreis jedoch jeweils über einen leistungsfähigen PC am Arbeitsplatz verfügt, macht hier der Einsatz von Terminal Services für interne Mitarbeiter keinen Sinn.

Die Rechenleistung der PCs würde nicht genutzt und stattdessen wäre eine hohe Belastung des Servers durch ressourcenintensive Programme wie *OPTISIM* die Folge.

Lokal installierte Anwendungen konnten nicht im Portal unterstützt werden, da keine hybride Lösung aus Terminal Services und automatischer Softwareverteilung (vgl. Softgrid und ZeroTouch in Kapitel 3.3) verfügbar war. Somit wurde die Zielgruppe des Prozess Design Portals vorerst allein auf externe Nutzer beschränkt.

6.4.2 Portalserver

Der Begriff Portal wird sehr häufig verwendet und besitzt dabei nicht immer die gleiche Bedeutung. Im Fall von Linde ist eine Applikation gemeint, welche, basierend auf Webtechnologien, einen zentralen Zugriff auf personalisierte Inhalte sowie bedarfsgerecht auf Prozesse und Dienste bereitstellt. Charakterisierend für Portale ist die Integration von heterogenen Anwendungen, Daten und Umgebungen auf einer Portalplattform (vgl. KG04).

Viele dieser Punkte sind beim Prozess Design Portal erfüllt, womit die Bezeichnung Portal gerechtfertigt ist. Es werden Anwendungen und Inhalte auf einer web-basierenden Plattform integriert und, je nach Gruppe, wird das Angebot angepasst.

Anbieter wie IBM, SUN, Oracle und viele andere bieten für diesen Zweck eigene Produkte, so genannte Portalserver an. Sie benutzen fast ausschließlich die Portlet Technologie. Portlets sind in Java geschriebene Komponenten und basieren auf dem Portlet Container, vergleichbar mit Servlets, die sich vom Servlet Container ableiten.

Portlets sind eigentlich die Fenster, aus denen sich das Portal zusammensetzt (vgl. HH03). Dabei können Portlets ganz unterschiedliche Aufgaben übernehmen, wie das Anzeigen der Mailbox oder von Dateien in einem bestimmten Serververzeichnis (siehe Abbildung 6.1). Es gibt viele vorgefertigte Portlets für verschiedene Anwendungen wie z.B. Lotus Notes, Microsoft Exchange und eben auch für das Citrix Webinterface.

Portalserver bieten eine unüberschaubar große Zahl von Einstellungsmöglichkeiten an. Neben Anpassungen des Layouts spielt die Personalisierung der Oberfläche eine besonders wichtige Rolle. Die Abteilung Human Resources benötigt ganz andere Informationen wie z.B. der Einkauf. Mit Portalservern lässt sich das Erscheinungsbild für die unterschiedlichen Benutzergruppen anpassen. Darüber hinaus kann jeder Benutzer das Portal den eigenen Bedürfnissen anpassen. Er kann beispielsweise Dienste hinzufügen oder entfernen und seine Einstellungen in einem Profil speichern.



Abb. 6.1: Beispiel einer Portal Oberfläche an Hand des
Oracle Portal Servers. Quelle: Oracle

Der Portalserver übernimmt ebenfalls die komplette Durchsetzung und Verwaltung von Sicherheitsrichtlinien. Es kann sehr granular eingestellt werden welche Benutzer Zugang zu welchen Ressourcen erhalten sollen (vgl. [Ora06](#)).

Das Prozess Design Portal könnte also mit einem Portalserver umgesetzt werden. Das schon existierende Portlet für das Citrix Webinterface könnte genutzt werden, um die Applikationen anzuzeigen, während die Zusatzinformationen mit Hilfe von selbst erstellten Portlets auf die Plattform gebracht werden. Durch die Flexibilität und die nahezu unbegrenzte Zahl an Möglichkeiten des Portalserver, wäre die Lösung auch zukunftssicher gewesen.

Die Entscheidung fiel allerdings gegen eine Lösung mit einem Portalserver. Dafür gab es mehrere Gründe. Zum einen wurde bei Linde Engineering schon einmal versucht, im Rahmen einer anderen Diplomarbeit, den IBM *Websphere Portal Server* aufzusetzen und dabei wurden eher schlechte Erfahrungen mit diesem Produkt gemacht. Die Hardwareanforderungen sind sehr hoch, die Installation, Inbetriebnahme und Wartung einer solchen Lösung sind ebenfalls aufwendig.

Hinzu kommen noch sehr hohe Kosten von durchschnittlich ca. 10.000 Euro für die Serverlizenz und zusätzlich ca. 150 Euro pro Benutzerlizenz. Um Portlets entwickeln zu können, sind sehr gute Kenntnisse in Java notwendig. Da der Einsatz eines Portalserver einer Insellösung bei Linde Engineering gleichgekommen wäre, hätten bei Problemen die entsprechenden Ansprechpartner gefehlt und die Übergabe der Plattform hätte sich schwierig gestaltet. Von den angebotenen Funktionen wären im Rahmen des Prozess Design Portals nur ein Bruchteil wirklich zum Einsatz gekommen, weswegen eine Lösung mit einem Portalserver als überdimensioniert erschien.

6.4.3 Webserver

Die Alternative zu einem Portalserver ist eine klassische Webanwendung, die das Citrix Webinterface in irgendeiner Form integriert. Das Citrix Webinterface läuft ausschließlich auf Microsofts IIS (=Internet Information Services) Server. Der IIS Server ist im Windows Server integriert und kann statische HTML Seiten oder dynamische Seiten, die entweder mit den Microsoft Sprachen ASP bzw. ASP.NET oder mit Skriptsprachen wie PHP oder PERL erstellt wurden, hosten (vgl. [Wik06](#)).

Allerdings können mit IIS keine Java Servlets bzw. Java Server Pages gehostet werden. Um eine webfähige J2EE Applikation in Produktion zu bringen, muss ein Java-fähiger Webserver, wie z.B. Apache *Tomcat* oder der bei Linde bevorzugten IBM *Websphere Application Server*, eingesetzt werden.

Da die Entscheidung, wie im nächsten Kapitel [6.4.4](#) beschrieben, für Java getroffen wurde, musste eine Möglichkeit gefunden werden, den IIS Server mit dem Java Webserver kommunizieren zu lassen. Vom Webinterface mussten Daten, wie z.B. der Name einer auf Citrix gestarteten Anwendung, an die Java-Applikation übergeben werden, um die richtigen Zusatzinformationen zu dieser Anwendung anzeigen zu können.

Letztendlich kam eine Umleitung vom IIS Server zum Java Webserver zum Einsatz. Requests an den IIS Server, die bestimmten Regeln entsprechen, wie z.B. die Dateierweiterung .jsp oder eine bestimmte URL Pfadangabe, werden an den Java Webserver umgeleitet. Dieser bearbeitet den Request und schickt den dynamisch erstellten HTML Code zurück an den IIS Server zur Anzeige.

Beim IIS Server muss dafür mit Hilfe des Internet Server Application Programming Interface (=ISAPI) die Umleitung eingerichtet und der entsprechende Typ des Requests registriert werden (vgl. [IBM06](#)).

Diese Lösung stellte sich als praktikabel für das Projekt heraus. Die Entscheidung, welcher Java Webserver für das Hosten der J2EE Applikation verwendet werden sollte, traf im Grunde genommen das Data. Bei Linde existierten mehrere *Websphere Application Server*. Es gab bereits viel Erfahrung damit und alle wichtigen Punkte wie z.B. die Sicherheit waren schon ausgiebig behandelt worden. Ein weiterer Webserver wie z.B. *Tomcat* hätte in der Produktionsumgebung keine Unterstützung bei auftretenden Fehlern gehabt.

Das Prozess Design Portal sollte auch nicht auf einem eigenen Server laufen, sondern die Möglichkeit nutzen, in einer virtuellen Serverumgebung mit anderen Applikationen auf der gleichen physikalischen Maschine zu laufen. Damit konnten die Lizenzkosten für einen eigenen *Websphere Application Server* der Version 6 eingespart werden.

6.4.4 Java

Java ist eine objektorientierte Programmiersprache und als solche ein eingetragenes Warenzeichen der Firma Sun Microsystems. Java-Programme werden in einer speziellen Java-Laufzeitumgebung ausgeführt, deren wichtigster Bestandteil die Java Virtual Machine ist (vgl. [GWM01](#), S.40 f.).

In der Spezifikation J2EE (=Java 2 Platform Enterprise Edition) werden Softwarekomponenten und Dienste definiert, die primär in der Programmiersprache Java erstellt werden. Darin enthalten sind auch das Servlet API und Java Server Pages, mit denen es möglich ist, eine Anwendung für das Web zu erstellen (vgl. [Mic06b](#)).

Servlet bzw. *HttpServlet* ist eine Klasse, die vom vorgegebenen Servlet Container Eigenschaften und Methoden erben. Die wichtigsten Methoden sind dabei die unterstützten *doGet*- und *doPost*-Methoden, die HTTP Requests annehmen, eine oder mehrere Operationen ausführen und eine HTTP Response zurückschicken können (vgl. [GWM01](#), S.720).

Dabei lassen sich Servlets, ähnlich wie Skriptsprachen PHP und PERL, für die dynamische Erstellung von Webseiten nutzen, allerdings mit dem Vorteil der Integration mit gegebenenfalls schon vorhandenen J2EE Komponenten, wie z.B. Sicherheit

und Authorisierung. Ein deutlicher Unterschied zu den Skriptsprachen ist, dass kein Parser zum Einsatz kommt. Stattdessen wird das Servlet kompiliert und bleibt im Speicher während den Requests.

Mit den Java Server Pages kann das Model-View-Controller Konzept umgesetzt werden. Sie dienen hauptsächlich der Darstellungslogik bzw. dem "View" Teil der Webapplikation, während die Servlets die Rechenlogik bzw. den "Controller" Teil abdecken. Tatsächlich werden aus den Java Server Pages in einem internen Prozess Servlets generiert. Der Vorteil bei Java Server Pages liegt im leichten Umgang mit HTML Quellcode. Während bei Servlets jegliche HTML Ausgabe über eine Funktion generiert wird, kann bei Java Server Pages, wie bei einer gewöhnlichen HTML Seite, HTML Code verwendet werden. Zusätzlich sind sogenannte Scriptlets, also Programmabläufe innerhalb definierter Bereiche, erlaubt (vgl. [U1105](#), S.1102).

Die Entscheidung für die Verwendung von Java bzw. Servlets und Java Server Pages wurde maßgeblich durch die umfangreiche Nutzung innerhalb von Linde Engineering beeinflusst. Andere Abteilungen innerhalb des Bereiches Informatik betreiben bereits komplexe J2EE Applikationen. Damit stehen bei Fragen immer erfahrene Entwickler zur Verfügung. Da die Wartung nach der Übergabe des Prozess Design Portals so einfach wie möglich gehalten werden sollte, kam eine andere Programmiersprache, mit der es wenig Erfahrungen gibt, eigentlich nicht in Frage.

Ein weiteres Argument für Java war der Einsatz des bei Linde entwickelten DfWeb Frameworks. Mit DfWeb wurde mit Hilfe von Klassen und Tag Libraries die Darstellung von Daten aus verschiedenen Quellsystemen in einer Webapplikation vereinfacht. Der Fokus des Einsatzes lag dabei beim "Project Data Portal", bei dem alle wichtigen Daten eines Projektes eingesehen werden konnten. DfWeb wurde innerhalb des Projektes für die Erstellung der Stoffdatenlisten verwendet.

6.5 Umsetzung

Nachdem alle Möglichkeiten abgewogen wurden, fiel die Entscheidung für eine Java Webapplikation, die auf einem IBM *Websphere Application Server* laufen und das Citrix Webinterface integrieren soll.

Damit wurde die langfristige Ausrichtung, mit einer Citrix Umgebung zu arbeiten, gefestigt und der Vorgabe anderer Abteilungen bzw. der Informatik Strategie für den Einsatz von Java und *Websphere* Rechnung getragen.

Während des gesamten Projektes war eine enge Zusammenarbeit mit dem Data Center bei Linde in Pullach erforderlich, da der Testserver, sowie die produktive Umgebung von dort aus administriert werden soll. Es waren also mit der lokalen Entwicklungsumgebung, der Testumgebung und der produktiven Umgebung drei unterschiedliche Stufen im Entwicklungsprozess notwendig.

Für die produktive Umgebung spielte besonders die Sicherheit beim Zugang und der Zugriff des Portals auf Ressourcen eine tragende Rolle. Da die Applikation auf das Intranet und wissenskritische Daten zugreift, war die Voraussetzung für den Zugriff von außerhalb des Firmennetzwerkes, der Einsatz einer starken Authentisierung mittels *SecurID* Karte.

Für die Entwicklung des Prozess Design Portals musste eine lokale Entwicklungsumgebung eingerichtet werden. Zu Testzwecken war dies vorerst ein IIS Server mit Citrix Webinterface und ein Apache *Tomcat* Server für die Java Applikation, die beide auf einer Maschine liefen. Nach mehreren Treffen mit Verantwortlichen aus dem Data Center wurde die lokale Entwicklungsumgebung der Testumgebung und der produktiven Umgebung im Datenzentrum angeglichen und der *Tomcat* Server mit der IBM *Rational Software Development Platform* (siehe Abbildung 6.2) inklusive *Websphere* Applikationsserver ausgetauscht.

Das Citrix Webinterface ist in der *Access Suite*, die von Linde lizenziert wurde, enthalten. Es handelt sich dabei um eine ASP.NET Applikation, die auf dem IIS Server gehostet wird. Das Webinterface ist im Grunde genommen eine webfähige *Program Neighborhood*, die alle für den Benutzer auf dem *Presentation Server* freigegebenen Anwendungen anzeigt und die Verbindung zwischen Client und Server einleitet.

Es existiert eine leider nicht ausreichende Dokumentation von Citrix, wie das Webinterface auf die Bedürfnisse der Firma angepasst werden kann. Wichtige Punkte sind dabei das Layout, Fehlermeldungen, Texte, sowie Verhalten bei Login oder Logout. Das Webinterface kann mit der Citrix Management Console verwaltet und konfiguriert werden. Es können z.B. grobe Einstellungen zur Darstellung oder zur Art der Authentifizierung vorgenommen werden.

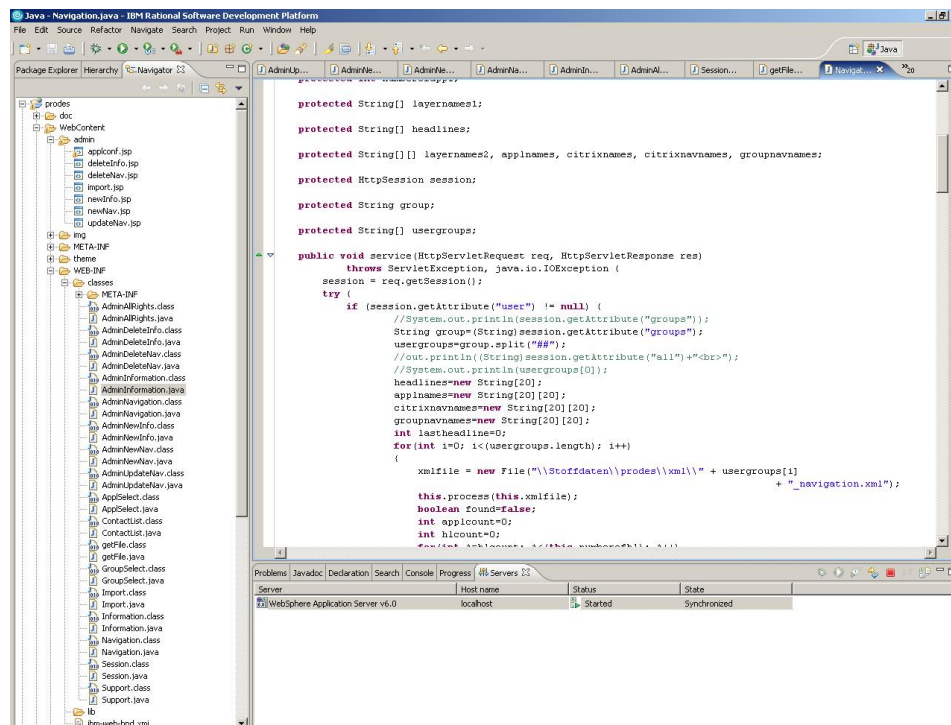


Abb. 6.2: Die IBM Rational Software Development Platform mit dem Websphere Application Server 6

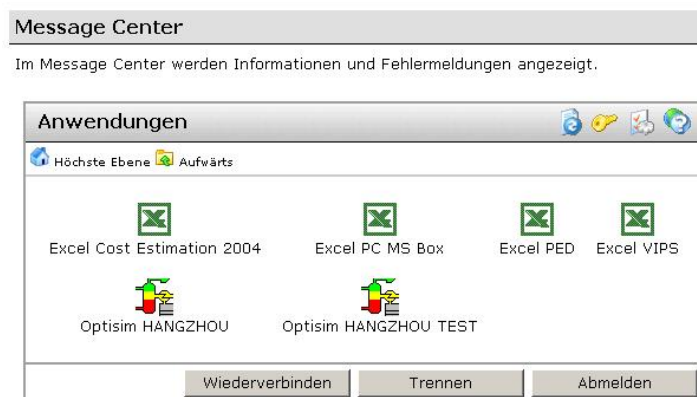


Abb. 6.3: Das Citrix Webinterface vor der Anpassung an das Corporate Design

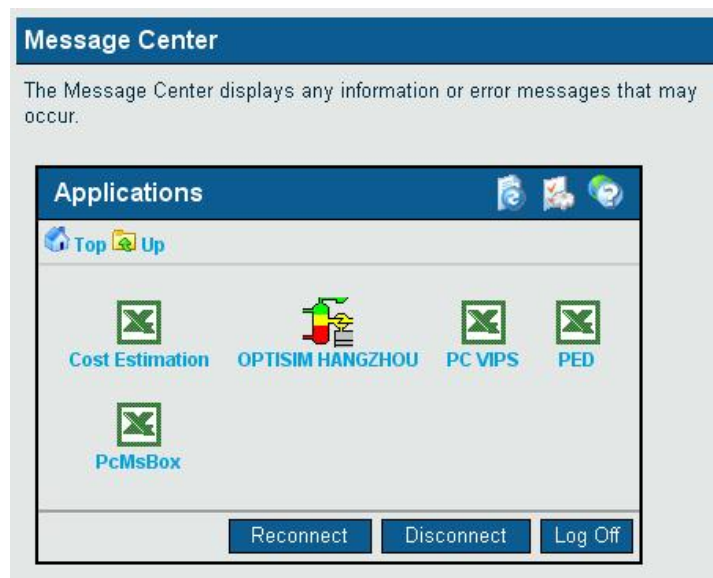


Abb. 6.4: Das Citrix Webinterface nach der Anpassung des Layouts

Der *Presentation Server* mit allen Applikationen, Gruppen und Rechten wird bei Linde vom Data Center verwaltet. In der Abteilung IV gibt es daher keine direkte Möglichkeit Anwendungen hinzuzufügen, zu löschen, einer Gruppe Rechte zuzuweisen oder zu entziehen. Somit konnte kein direkter Einfluss auf den Inhalt, der vom Webinterface angezeigt wird, genommen werden.

Das Layout bei Linde ist in einem eigenen Portal zum Corporate Design sehr detailliert festgelegt. Auf einer Seite im Intranet lassen sich alle Regeln zur Gestaltung von Print Anzeigen, Präsentationen, Publikationen u.ä. abrufen. Die Farbgebung, die Schriftarten, Schriftform und Abstände waren somit vorgegeben und wurden auf das Prozess Design Portal übertragen. Davon war zum einen die Java Applikation bzw. die generierten HTML Seiten betroffen, zum anderen auch das Webinterface, an dem einige Änderungen im Erscheinungsbild vorgenommen werden mussten (siehe Abbildung 6.3 und 6.4).

Von der Tatsache, dass es sich beim Webinterface und beim Java Teil des Portals um getrennte Applikationen handelt, die sogar auf unterschiedlichen Servern laufen, sollten die Benutzer nichts mitbekommen. Ein resultierendes Ziel war deshalb eine möglichst nahtlose Integration des Webinterfaces in das Prozess Design Portal.

Mit Hilfe von Frames wurden beide Teile gekoppelt, wobei es möglich sein sollte

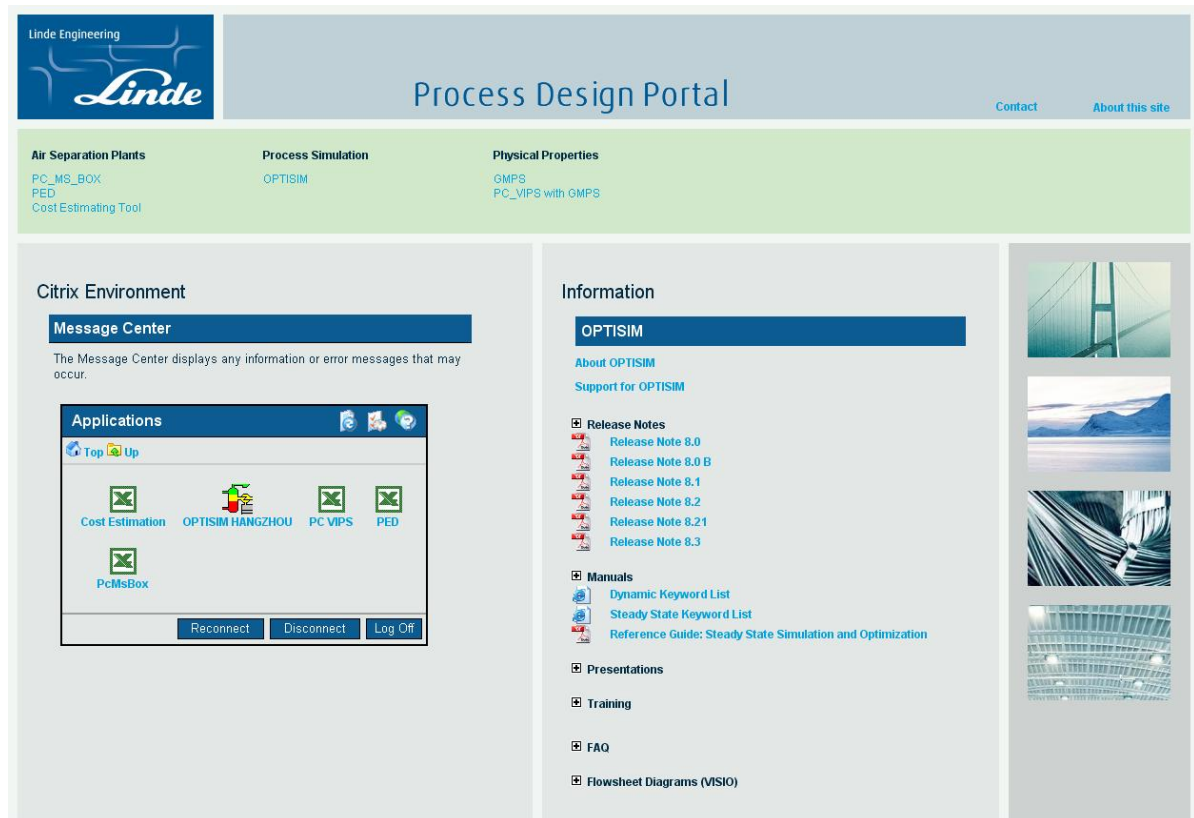


Abb. 6.5: Screenshot des Prozess Design Portals

Daten vom Webinterface Frame, wie z.B. den Namen der gestarteten Applikation, an den Java Frame per Java Skript zu übergeben. Damit konnten beim Start einer Applikation gleichzeitig alle wichtigen zusätzlichen Informationen angezeigt werden. Für die Übergabe von Parametern mit Java Skript mussten Methoden und Klassen des Webinterface angepasst werden. Z.B. wurde die Methode für den Aufruf der Startskripts einer Applikation erweitert. So wird der Name der Anwendung an ein Java Servlet auf dem *Websphere* Server weitergegeben.

Um die Übergabe von Parametern mit Java Skript zu ermöglichen, musste das Prozess Design Portal über einen Servernamen und Port ansprechbar sein, da sonst Sicherheitsmechanismen im Browser die Übergabe von Parametern unterbinden (Warnung wegen Cross Site Scripting). Zu diesem Zweck wurde eine Umleitung von Java Requests vom IIS Server auf den *Websphere* Server eingerichtet (siehe Abbildung 6.6). Mittels eines Plugins werden HTTP Requests, die die Java Applikation betreffen, vom IIS weitergeleitet, vom *Websphere* Server abgearbeitet und der generierte HTML Quellcode zurück an den IIS Server zur Anzeige geschickt. Damit ist es möglich das Webinterface und die Java Applikation beide unter dem IIS Servernamen und Port anzusprechen.

Der Java Teil des Prozess Design Portals besteht aus der Navigation, der Anzeige von Zusatzinformationen und einem Administrationsbereich, in dem festgelegt werden kann, welche Gruppen Zugriff auf zugeordnete, zusätzliche Informationen erhalten. Anhand der Einstellungen für jede Gruppe werden auf der Seite für den Benutzer, je nach Zugehörigkeit, unterschiedliche Navigationspunkte und Informationen angezeigt (siehe Abbildung 6.7).

Die Datenspeicherung für die Applikationen wurde mit Hilfe von XML Dateien umgesetzt. In den XML Dateien wurden mit den Java Servlets und mit Hilfe der externen *Xerces* Bibliothek die Rechte der einzelnen Gruppen strukturiert hinterlegt bzw. ausgelesen. Dadurch war keine Anbindung an eine Datenbank nötig, wodurch vermutlich künftig auftretende Serverwechsel viel einfacher vonstatten gehen können.

Eine Anforderung war es, ganz unterschiedliche Arten von Inhalten in das Prozess Design Portal einbinden zu können. Deshalb wird nicht nur das Hochladen und Verlinken von allen erdenklichen Dateiformaten auf den Server unterstützt, sondern auch die Anbindung von externen Daten durch das Setzen von Links ins Internet oder

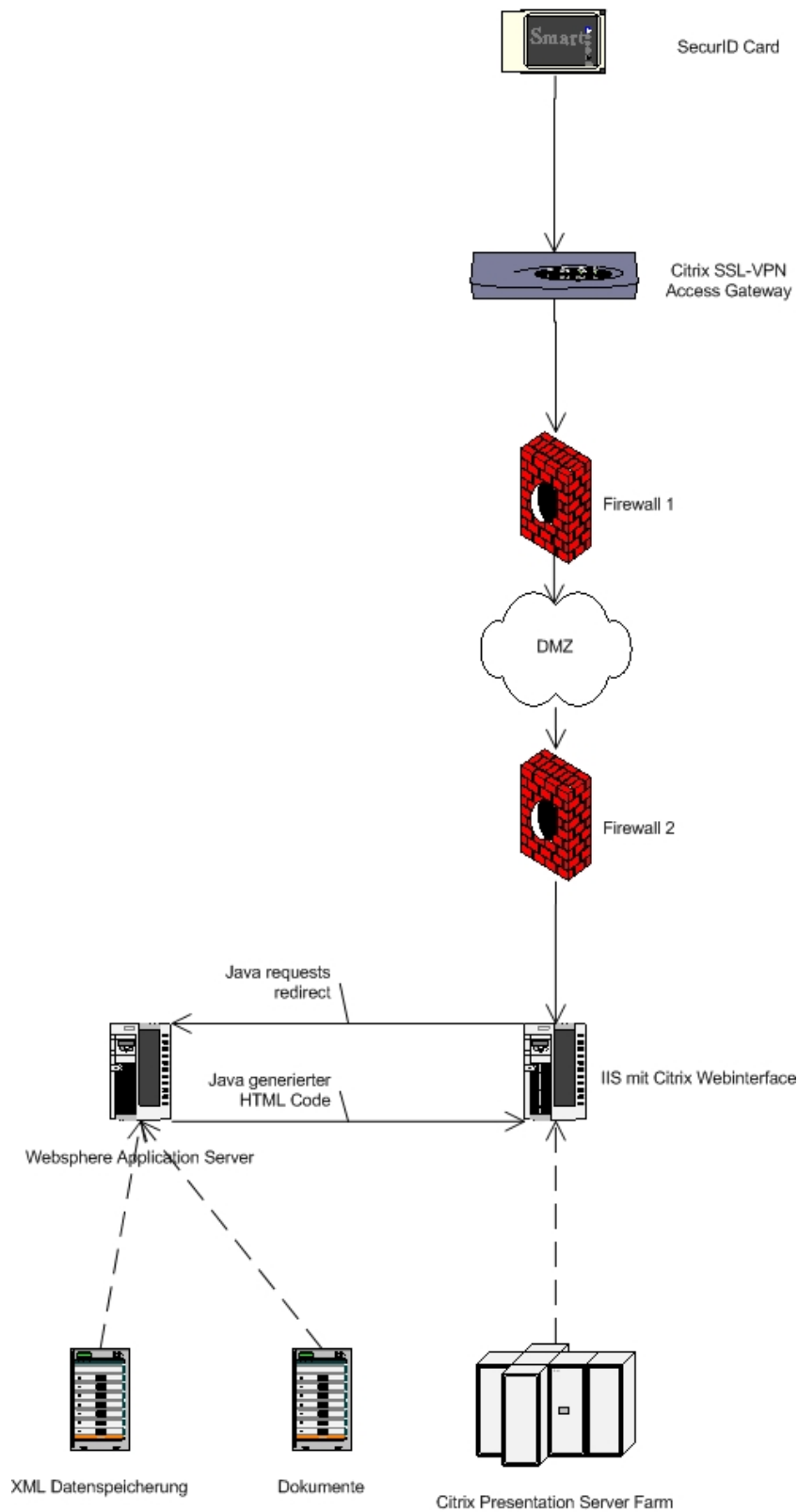


Abb. 6.6: Die Netzwerkarchitektur für den laufenden Betrieb des Prozess Design Portals bei Linde

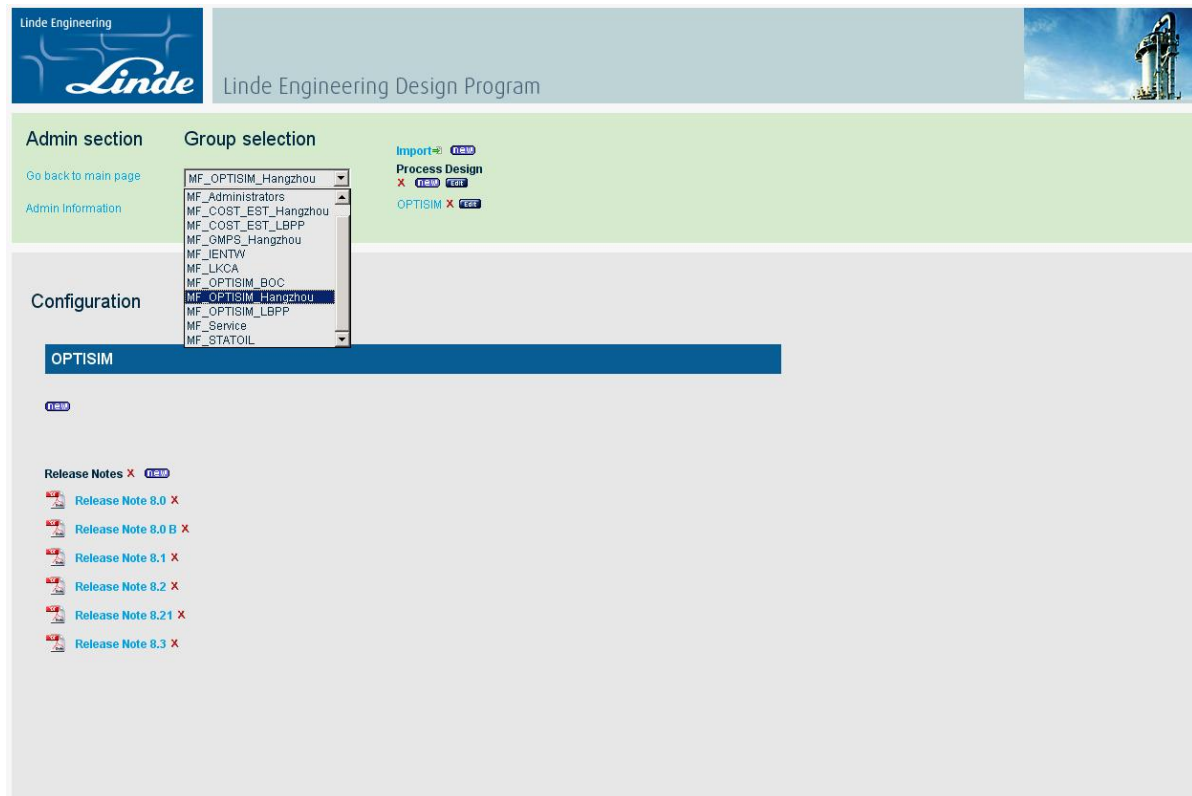


Abb. 6.7: Screenshot des Administrationsbereiches des Prozess Design Portals

Intranet. Damit ist die Plattform so flexibel und skalierbar wie möglich gehalten, um auch zukünftige Änderungen oder Erweiterungen zu unterstützen.

Eine Herausforderung war die komplizierte Verwaltung von Ressourcen bzw. die fehlende Transparenz, welche Gruppen Zugriff auf welche Ressourcen besitzen. Dafür gab es zwei hauptsächliche Gründe. Zum einen wird die Administration von Anwendungen und Gruppen für den *Presentation Server* vom Data Center durchgeführt und für Mitarbeiter der IV Abteilung ist es nur umständlich einzusehen, welche Rechte die einzelnen Gruppen besitzen. Zum anderen existieren neben der Gruppenverwaltung für Applikationen bei Citrix noch andere Verwaltungsmechanismen, wie z.B. die direkte Rechtevergabe für Gruppenlaufwerke und Dateien auf Netzwerk Laufwerken. Der Zugriff auf Stoffdaten wird z.B. anhand von Sicherheitseinstellungen von Dateien geregelt. Diese Lösung war sehr unübersichtlich und Änderungen kompliziert durchzuführen.

The screenshot shows the 'Physical Properties Portal' interface. On the left is a navigation menu with options like Homepage, Components, Groups, Classes, Fragments (highlighted), Methods, Method parameters, Properties, References, and Units. The main area displays a table of fragments. At the top of the table, there are search filters for 'No:', 'Synonym No:', and 'Name:'. The table has columns: Line, No, Synonym No, Name, Length, and Length 2. It lists 20 fragments, including properties like Molecular Weight, Critical Temperature, and Normal Boiling Point. Below the table, there is a 'Display' dropdown set to 20 of 220 items, and a 'Global Navigation' bar at the bottom with links to various sections of the portal.

Line	No	Synonym No	Name	Length	Length 2
1	101	1	MOLECULAR WEIGHT	1	
2	101	2	MOLWT	1	
3	101	3	MW	1	
4	201	1	CRITICAL TEMPERATURE	1	
5	201	2	TC	1	
6	301	1	CRITICAL PRESSURE	1	
7	301	2	PC	1	
8	401	1	CRITICAL VOLUME	1	
9	401	2	VC	1	
10	501	1	CRITICAL DENSITY	1	
11	501	2	RHOC	1	
12	601	1	CRITICAL COMPRESSIBILITY	1	
13	601	2	ZC	1	
14	701	1	ACENTRIC FACTOR	1	
15	701	2	OMEGA	1	
16	901	1	LIQUID MOLAR VOLUME AT NORMAL B P	1	
17	901	2	MOLAR VOLUME	1	
18	901	3	MOLVOL	1	
19	901	4	VB	1	
20	1001	1	NORMAL BOILING POINT	1	

Abb. 6.8: Applikation zur Anzeige der Stoffdaten mit Hilfe des DfWeb Frameworks

Nach einer Analyse des aktuellen Zustandes und der Anforderungen wurde klar, dass es sich bei einer Administrationsplattform, mit der alle Ressourcen verwaltet werden können, im Umfang um ein eigenständiges Projekt handelt. Es konnten deshalb, neben den Zugriffsrechten zu Zusatzinformationen für Applikationen, keine weiteren Administrationsmöglichkeiten beim Prozess Design Portal implementiert werden.

Bei den Stoffdatenlisten (siehe Abbildung 6.8) handelt es sich um Daten aus einer Oracle Datenbank, die in einer Listenform im Prozess Design Portal angeboten werden sollten. In der Vergangenheit wurden diese Listen direkt aus der Datenbank mit einer Abfrage geholt. Um die Übersichtlichkeit zu steigern, sowie Sortier- und Filterfunktionen anzubieten, sollten die Daten anwenderfreundlich über den Browser aufrufbar sein.

Da der verbesserte Aufruf der Stoffdaten eine große Bedeutung hatte, wurde im Rahmen der Erstellung des Prozess Design Portals eine weitere Java Applikation

erstellt, die mit Hilfe des DfWeb Frameworks die Daten in Listenform im Browser darstellbar macht. Das DfWeb Framework wurde von Linde entwickelt und kapselt in Controllerklassen grundlegende Funktionalitäten wie u.a. die Datenbankanbindung, das Sessionmanagement oder die Zugriffssicherheit. Der Entwickler kann durch das Erstellen einfacher JSP Seiten und mit Hilfe von Tag Libraries auf sonst nur zeitintensiv zu entwickelnde Funktionalitäten wie Sortiermechanismen und Filterregelungen zurückgreifen. Die Stoffdatenlisten wurden auf einem eigenen *Websphere* Server gehostet und in das Prozess Design Portal verlinkt.

Gemäß den Vorgaben wurden die lokal entwickelten Applikationen zuerst in eine Testumgebung bei Linde portiert. Da die Testumgebung der produktiven Umgebung angepasst ist, sind Applikationen, die ohne Fehler in der Testumgebung laufen, auch in der produktiven Umgebung lauffähig. In der Testumgebung wurde ein letzter Test auf Fehler und Bugs durchgeführt, bevor die Webanwendung schließlich in Produktion ging und das Projekt damit abgeschlossen wurde.

Kapitel 7

Fazit

Terminal Services sind ein ausgereiftes Konzept um Benutzern Anwendungen zentral auf dem Server bereitzustellen. Ob sich der Einsatz von Terminal Services lohnt, hängt von Faktoren wie der Anzahl und Sitz der Benutzer, Anzahl und Art der Anwendungen und den Anforderungen im Unternehmen ab.

Gerade wenn Wartungszeiten für die Rechner der Benutzer und für die Pflege von Applikationen verkürzt und damit die Kosten gesenkt werden sollen, die Client Rechner länger benutzt werden sollen oder ein Umstieg auf Thin Clients geplant ist, sind Terminal Services der richtige Weg. Im praktischen Beispiel bei Linde haben sich die Mobilität bei der Benutzung, der weltweite Zugriff von verteilten Standorten und der Sicherheitsaspekt, dass Anwendungen das Unternehmen nicht verlassen, als ausschlaggebende Kriterien für die Beibehaltung einer Citrix Umgebung herausgestellt.

Wenn andere Aspekte, wie die bessere Rechenleistung, die größere Freiheit bei der Benutzung oder die Möglichkeit zum Offline Betrieb verwirklicht werden sollen, ist eine traditionelle Lösung, bei der jeder Benutzer einen PC mit eigenen Installationen der Anwendungen erhält bzw. ein automatisches Verteilen der Anwendungen mit Hilfsprogrammen wie SMS, vorzuziehen.

Die besprochenen neuen Entwicklungen wie Virtualisierung und Blades helfen bei der Skalierung von großen Terminal Serverfarmen. Neue Konzepte, wie virtualisierte Desktops und Bladed PCs, können als Zwischenlösungen von Terminal Services und traditionellen PCs angesehen werden. Diese Konzepte verbinden einige Vorteile beider Lösungen.

Ob sich virtuelle Desktops oder Bladed PCs in größerem Maße durchsetzen, bleibt abzuwarten.

Applikationsvirtualisierung, sowie die Verbesserung beim Zugang zu den Anwendungen über das Internet durch höhere Sicherheit und intelligentere Zugangskontrollen, sind wichtige aktuelle Entwicklungen bei Terminal Services. Sie lösen zum einen das Problem von Applikationskonflikten und sprechen zum anderen für den Einsatz von Citrix Umgebungen bei der Bereitstellung von Applikationen im Internet.

Durch das in Kürze erscheinende Windows Vista bzw. Longhorn Server Betriebssystem von Microsoft ergibt sich eine neue Ausgangslage auf dem Markt für Terminal Services, in der es für Zusatzanbieter immer schwieriger wird, Kaufanreize gegenüber dem Basisprodukt von Microsoft zu erzeugen. Die neue Präsentationsschicht von Windows Vista bzw. die Beschreibung des Bildschirminhaltes mittels XAML könnte die Funktionsweise von Terminal Services in Zukunft grundlegend verändern.

Es ist absehbar, dass es auf Grund der Übernahmen von Citrix voraussichtlich zu einer Verbesserung des Load Balancing durch Daten über die Performanz der Benutzer Sessions und zu einem weiteren Vorstoß in den Markt für Netzwerkhardware kommen wird.

Im praktischen Teil der Arbeit im Geschäftsbereich Linde Engineering der Linde AG wurde erkennbar, welche Anforderungen mit einer Citrix Umgebung abgedeckt werden können und wie der laufende Betrieb einer webfähigen Lösung mit dem Webinterface aussehen kann.

Auf Basis der Untersuchung und Bewertung von Alternativen wurde eine Portal Seite erstellt, die mit dem Einsatz von Citrix, dem Websphere Server und Java als Programmiersprache zukunftsfähig ist, und mit der die Anforderungen in einem sinnvollen Kosten-Nutzen-Verhältnis erfüllt werden. Über die neue Seite können die externen Nutzer weltweit effizienter auf die Prozess Design Programme und wichtige Informationen zugreifen.

Neben den Gründen für eine Beibehaltung der Citrix Umgebung, wurde die Integration des Webinterfaces in das Prozess Design Portal beschrieben und die Funktionsweise erläutert.

Abbildungsverzeichnis

2.1	Der Markt für Terminal Server entwickelte sich seit der ersten Veröffentlichung von Microsoft hervorragend. Quelle: Zona Research	10
2.2	Mit dem Web Client für Terminal Server kann der Benutzer eine Remote Desktop Umgebung im Browser starten. Quelle: Windows IT Pro	13
2.3	Die Komponenten des Terminal Servers. Quelle: (MO03)	18
2.4	Der Session Manager verwaltet die aktuellen Verbindungen zum Terminal Server. Quelle: (MO03)	19
2.5	Mit Hilfe von virtuellen Kanälen lassen sich Daten in einer RDP Sitzung austauschen. Quelle: (MO03)	21
2.6	Bei einer zentralen Architektur wird die Bandbreite mit der Datenübertragung belastet. Quelle: (MO03)	24
2.7	Bei einer dezentralen Architektur läuft nur das Präsentationsprotokoll über das WAN. Quelle: (MO03)	25
2.8	Jedem Terminal Server sollte ein Lizenzserver zugeordnet sein um einen schnellen Zugriff zu gewährleisten. Quelle: (MO03)	26
2.9	Studien belegen anhand der TCO die Einsparungen bei der Nutzung von Terminal Services anstatt traditioneller PCs. Quelle: ETCF	27
2.10	Mit Smooth Roaming können Benutzer zwischen verschiedenen Endgeräten wechseln, ohne ihre Session beenden zu müssen. Quelle: Citrix	33
3.1	VMWare Server benötigt wie der Microsoft Virtual Server ein Wirt-Betriebssystem auf dem die virtuellen Maschinen laufen. Quelle: VMWare	39

3.2	Beim <i>ESX Server</i> laufen die virtuellen Maschinen ohne Wirt-Betriebssystem direkt auf dem Rechner. Quelle: VMWare	39
3.3	Bei virtuellen Desktops können mehrere Benutzer auf einem Server in ihrer eigenen virtuellen Umgebung arbeiten. Quelle: VMWare	41
3.4	Vergleich der Architektur von VDI (links) mit der eines Terminal Servers (rechts). Quelle: Brian Madden	42
3.5	Bei einer traditionellen Installation hat die Anwendung Zugriff auf Komponenten des Betriebssystems. Quelle: Softricity	43
3.6	In einer virtuellen Umgebung hat die Applikation keinen schreibenden Zugriff auf das Betriebssystem. Quelle: Softricity	44
3.7	Beispiel für ein Blade: HP ProLiant BL25p Server Blade. Quelle: HP	46
3.8	Ein PC Blade von ClearCube. Quelle: ClearCube	48
3.9	Das Chassis im Datenzentrum für die PC Blades. Quelle: ClearCube	48
3.10	Mit der Managementsoftware lässt sich der Zustand der Blades überwachen und Einstellungen vornehmen. Quelle: ClearCube	50
3.11	Mit dem Sequencer kann ein Anwendungspaket erstellt werden, das paketweise zum Client geschickt werden kann. Quelle: Softricity	51
3.12	Das erstellte Applikationspaket läuft beim Client in einer virtuellen Umgebung. Quelle: Softricity	52
3.13	Netzwerkarchitektur mit <i>Access Gateway</i> und AAC. Quelle: Citrix	57
3.14	Mit ACE lässt sich der Zugriff von externen Benutzern auf das Netzwerk regeln. Quelle: VMWare	59
3.15	Der Administrator kann bei ACE die genauen Berechtigungen für den Zugriff auf das Netzwerk festlegen. Quelle: VMWare	60
3.16	Vergleich der vorgestellten Lösungen zur Bereitstellung von Applikationen	61
5.1	Beispiel einer Chemie/Petrochemie Anlage. Quelle:Linde	72
6.1	Beispiel einer Portal Oberfläche an Hand des <i>Oracle Portal Servers</i> . Quelle: Oracle	81

6.2	Die IBM <i>Rational Software Development Platform</i> mit dem <i>Websphere Application Server 6</i>	86
6.3	Das Citrix Webinterface vor der Anpassung an das Corporate Design .	86
6.4	Das Citrix Webinterface nach der Anpassung des Layouts	87
6.5	Screenshot des Prozess Design Portals	88
6.6	Die Netzwerkarchitektur für den laufenden Betrieb des Prozess Design Portals bei Linde	90
6.7	Screenshot des Administrationsbereiches des Prozess Design Portals .	91
6.8	Applikation zur Anzeige der Stoffdaten mit Hilfe des DfWeb Frame- works	92

Literaturverzeichnis

- [BIT06] BITKOM. Software zum Mieten erlebt in Deutschland eine Renaissance, 2006. http://www.bitkom.org/39960_39933.aspx.
- [Bod05] Ulrich B. Boddenberg. *Microsoft-Netzwerke, Konzepte und Lösungen*. Galileo Press, 2005.
- [BS06] Jeffrey Burt and John G. Spooner. Chip Makers Pave the Way for Desktop Virtualization, 2006. <http://www.eweek.com/article2/0,1895,1926718,00.asp>.
- [Bur91] P.S. Burr. OPTISIM - Process Simulation and Optimization System, 1991. Linde AG.
- [C.H05] Verlag C.H.Beck. Die Linde AG, Geschichte eines Technologiekonzerns 1879-2004, 2005. <http://rsw.beck.de/rsw/shop/default.asp?docid=108492>.
- [Cit04] Citrix. Citrix Expands Its Access Infrastructure Leadership with Acquisition of Net6, Innovator in Secure Access Gateways, 2004. http://support.citrix.com/servlet/KbServlet/download/8541-102-14220/VPN_AdminGuide.pdf.
- [Cit05] Citrix. Citrix To Expand Access Platform with Acquisition of NetScaler, 2005. <http://www.citrix.com/English/NE/news/news.asp?newsID=20951>.
- [Cit06a] Citrix. Access Gateway Administrator's Guide 4.2 - German, 2006. <http://www.citrix.com/site/NE/news/news.asp?newsID=14851>.
- [Cit06b] Citrix. Über Citrix Systems, 2006. <http://www.citrix.de/index.cfm?E89A8D12B0684E28992ED3F4AC4E9E14>.

- [Cit06c] Citrix. Citrix Acquires Reflectent Software, Enhances and Extends Its Access Platform, 2006. <http://www.citrix.com/English/NE/news/news.asp?newsID=25118>.
- [Cit06d] Citrix. Project Constellation, A unique look into the future of application virtualization at Citrix..., 2006. http://www.citrix.com/lang/English/lp/lp_23669.asp.
- [Cle06] ClearCube. ClearCube, A Complete Business Computing Solution, 2006. http://www.clearcube.com/controller/product_overview.php.
- [Dre05] Carsten Dreyer. *Citrix Access Suite und Microsoft Terminal Services*. Redline GmbH, 2005.
- [EK06] Gabriele Engl and Andreas Kröner. Success Factors for CAPE in the Engineering Practice of a Process Plant Contractor, 2006. Computer-Aided Chemical Enigeering 21A, Seite 763-768.
- [For05] European Thin Client Forum. Die Perspektive: Der Thin Client-Markt bleibt eine Wachstumsbranche, 2005. http://www.etcf.de/cms/branche_zahlen_de/.
- [GM06] David Greschler and Brian Madden. Podcast: A conversation with Softricity co-founder David Greschler, 2006. <http://www.brianmadden.com/content/content.asp?id=585>.
- [Gru06] Lukas Grunwald. Frisch gebündelt, Softwareverteilung auf Serverfarmen, 2006. iX 07/06, Seite 94 bis 95.
- [GWM01] Joachim Goll, Cornelia Weiß, and Frank Müller. *Java als erste Programmiersprache, Vom Einsteiger zum Profi*. B.G. Teubner, 2001.
- [HH03] Stefan Hepper and Stephan Hesmert'. Introducing the Portlet Specification, Part 1, 2003. <http://www.javaworld.com/javaworld/jw-08-2003/jw-0801-portlet.html>.
- [Hül05] Ralph Hülsenbusch. Boxenstopp, Virtualisierte Server mit Egeneras Blade Frame, 2005. iX 09/05, Seite 50 bis 54.
- [Hül06] Ralph Hülsenbusch. Klingen kreuzen, Blade-Server fürs Rack, eine Übersicht, 2006. iX 05/06, Seite 106 bis 113.

- [HP06] Hewlett-Packard. HP Consolidated Client Infrastructure, 2006. <http://h71028.www7.hp.com/enterprise/cache/279997-0-0-225-121.aspx>.
- [IBM06] IBM. Configuring Microsoft Internet Information Services (IIS), 2006. http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tins_manualWebIIS.html.
- [Ige06] Igel. IGEL Technology, Clever Clienting, 2006. <http://www.igel.de/>.
- [KESL97] Andreas Köner, E. Eich-Söllner, and P. Lory. Stationary and dynamic flowsheeting in the chemical engineering industry, 1997. Surveys on Mathematics for Industry 7, Seite 1-28.
- [KG04] Anja Kirchhof and Thorsten Gurzki. Was ist ein Portal? Definition und Einsatz von Unternehmensportalen, 2004. <http://www.gurzki.de/publications/padem/Was%20ist%20ein%20Portal/>.
- [KH01] Bernd Kretschmer and Stephan Herkert. *Windows 2000 - Terminaldienste*. Addison-Wesley, 2001.
- [Lüd06] Nico Lüdemann. *Citrix Presentation Server 4, Grundlagen, Praxis, Referenz*. Galileo Press, 2006.
- [Lie06] Daniel Liebisch. Mobiles Arbeiten in Citrix-Umgebungen, 2006. http://www.computerwoche.de/produkte_technik/mobile_computing/573542/index.htm.
- [Lin02] Intranet Linde. Aufgabenbeschreibung IV, 2002.
- [Lin05a] Anlagenbau Linde. Anlagenbau, 2005. <http://www.linde-anlagenbau.de/anlagenbau/index.php>.
- [Lin05b] Group Linde. Corporate Heritage, 1975-2004. Aufstieg zum Global Player, 2005. http://www.linde.de/International/Web/Linde/likelindeger.nsf/docbyalias/page_ch_chronicle_19752004_detailoverview.
- [Lin05c] Group Linde. Der Linde Konzern, 2005. http://www.linde.de/international/web/linde/likelindeger.nsf/docbyalias/nav_lindegrou.

- [Mad02] Brian Madden. *Citrix MetaFrame XP, Advanced Technical Design Guide, Including Feature Release 2*. BrianMadden.com Publishing, 2002.
- [Mad03a] Brian Madden. Citrix and VMware: Past, Present, and Future (Part 1 of 3), 2003. <http://www.brianmadden.com/content/content.asp?ID=51>.
- [Mad03b] Brian Madden. Microsoft's Complete Longhorn Terminal Server Feature List, 2003. <http://www.brianmadden.com/content/content.asp?ID=38>.
- [Mad03c] Brian Madden. Point-Counterpoint: How Microsoft's Bear Paw will Affect Citrix, 2003. <http://www.brianmadden.com/content/content.asp?ID=38>.
- [Mad04a] Brian Madden. A Technical Analysis of Citrix's Application Streaming Announcement, 2004. <http://www.brianmadden.com/content/content.asp?ID=508>.
- [Mad04b] Brian Madden. Microsoft's Revised Windows Server 2003 Update Timeline, 2004. <http://www.brianmadden.com/content/content.asp?ID=221>.
- [Mad04c] Brian Madden. Will bladed PCs affect Citrix?, 2004. <http://www.brianmadden.com/content/content.asp?ID=160>.
- [Mad05a] Brian Madden. Citrix's New Marketing Message: There are three types of apps, we have three types of solutions, 2005. <http://www.brianmadden.com/content/content.asp?ID=509>.
- [Mad05b] Brian Madden. Podcast: Citrix and VMware - Current Scenarios and Future Direction, 2005. <http://www.brianmadden.com/content/content.asp?id=499>.
- [Mad05c] Brian Madden. What does Citrix's new 300M acquisition mean for the future of the company?, 2005. <http://www.brianmadden.com/content/content.asp?ID=465>.
- [Mad06a] Brian Madden. Citrix buys Application Performance Management vendor Reflectent. Is this a YAM?, 2006. <http://www.brianmadden.com/content/content.asp?ID=589>.

- [Mad06b] Brian Madden. Podcast: A talk about the future of Citrix and the Server-Based Computing Industry, 2006. <http://www.brianmadden.com/content/content.asp?id=590>.
- [Mad06c] Brian Madden. The facts about the Citrix Access Gateway, the Generic hardware it's built on, and running it in VMware, 2006. <http://www.brianmadden.com/content/content.asp?ID=558>.
- [Mic05] Sun Microsystems. Sun Microsystems Completes Tarantella Acquisition, 2005. <http://www.sun.com/smi/Press/sunflash/2005-07/sunflash.20050713.1.xml>.
- [Mic06a] Microsoft. Microsoft Extends Virtualization Strategy, Outlines Product Road Map, 2006. <http://www.microsoft.com/presspass/features/2006/may06/05-22Virtualization.msp>.
- [Mic06b] Sun Microsystems. Java EE At a Glance, 2006. <http://java.sun.com/javaee/index.jsp>.
- [MO03] Brian Madden and Ron Oglesby. *Terminal Services for Microsoft Windows Server 2003, Advanced Technical Design Guide*. BrianMadden.com Publishing, 2003.
- [MWM06] Tim Mangan, Phil Winslow, and Brian Madden. Podcast: A conversation about Microsoft buying Softricity: What it means now and for the future, 2006. <http://www.brianmadden.com/content/content.asp?id=599>.
- [OM06] Ron Oglesby and Brian Madden. Podcast: Interview with Ron Oglesby on Citrix, VMware, and mixing them together, 2006. <http://www.brianmadden.com/content/content.asp?id=579>.
- [Ora06] Oracle. Portal Center, Product Overview, 2006. <http://www.oracle.com/technology/products/ias/portal/index.html>.
- [PM06] Jeff Pitsch and Brian Madden. Podcast: A Conversation with Jeff Pitsch about Citrix Advanced Access Control, 2006. <http://www.brianmadden.com/content/content.asp?id=581>.
- [Sch05] Peter Schüler. Office aus dem Netz, 2005. Ct 01/05, Seite 178 bis 183.

- [Sch06a] Martin Schindler. XAML und WPF - Microsofts neue Geheimwaffen, 2006. http://www.silicon.de/enid/business_software/19930,3.
- [Sch06b] Kathrin Schmitt. Blades kommen (noch) ohne Standards aus, 2006. http://www.silicon.de/enid/client_server_host/16842.
- [Sch06c] Holger Schwichtenberg. Klassensprung, Microsofts WinFX-Erweiterung für .NET, 2006. iX 07/06, Seite 124 bis 130.
- [Sec06a] IT SecCity. Die Qual der Wahl: IPsec oder SSL?, 2006. http://www.itseccity.de/?url=/content/produkte/hintergrund/060131_pro_hin_watchguard.html.
- [Sec06b] RSA Security. RSA SecurID Authentication, 2006. <http://www.rsasecurity.com/node.asp?id=1156>.
- [Sof06a] Softricity. SoftGrid for Microsoft Systems Management Server (SMS), 2006. <http://www.softricity.com/products/softgrid-sms.asp>.
- [Sof06b] Softricity. Softricity Technology: Application Packaging with the Soft-Grid Sequencer, 2006. <http://www.softricity.com/products/sequencer.asp>.
- [Sof06c] Softricity. Softricity Technology: On-Demand Application Streaming, 2006. <http://www.softricity.com/products/delivery.asp>.
- [Sof06d] Softricity. Softricity ZeroTouch: IT Self-Service, 2006. <http://www.softricity.com/products/zerotouch.asp>.
- [Tei05] Petra Teichner. Thin Clients, Server Based Computing boomt - und niemand spricht darüber, 2005. http://www.silicon.de/enid/client_server_host/15744.
- [Tre03] Rod Trent. Distributing Software Using Microsoft Management Technologies, 2003. <http://www.microsoft.com/technet/prodtechnol/sms/sms2/dsumgmt.mspx>.
- [Tri03] Bernhard Tritsch. *Microsoft Windows Server 2003 Terminaldienste*. Microsoft Press Deutschland, 2003.

- [Tul05] Mitch Tulloch. Overview of Terminal Services, 2005. http://www.windowsnetworking.com/articles_tutorials/Overview-Terminal-Services.html.
- [Ull05] Christian Ullenboom. *Java ist auch eine Insel*. Galileo Press, 2005.
- [VMW06a] VMWare. The Assured Computing Environment for the Enterprise, 2006. <http://www.vmware.com/products/ace/>.
- [VMW06b] VMWare. VMware Virtual Desktop Infrastructure, 2006. <http://www.vmware.com/solutions/desktop/vdi.html>.
- [VMW06c] VMware. VMware VMotion, Migrate Virtual Machines with Zero Downtime, 2006. <http://www.vmware.com/products/vi/vc/vmotion.html>.
- [Web06] Thin Client Web. Was sind Thin Clients?, 2006. http://www.thin-client.info/thin_client/thinclient.html.
- [Wes04] Matthias Wessner. Mit oder ohne Aufsatz, Microsoft Windows 2003 vs. Citrix Metaframe XPe, 2004. iX 02/04, Seite 78 bis 82.
- [Wik06] Wikipedia. Comparison of web servers, 2006. http://en.wikipedia.org/wiki/Comparison_of_web_servers.
- [Wys06] Wyse. Wyse Thin Computing Hardware, 2006. <http://www.wyse.com/products/hardware/>.
- [Zie06] Michael Ziegler. Desktop zentral, VMWares Konzept der Virtual Desktop Infrastructure, 2006. iX 08/06, Seite 110 bis 111.